

n. 52
www.hackerjournal.it

Il SOFTWARE per scoprire se sei un VERO HACKER

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

RISPARMIARE
Basta farci spillare soldi da Epson

Symantech
test senza peli sulla lingua



QUATTORDICINALE ANNO 3
3 GIUGNO 2004 - 17 GIUGNO 2004
SPED. IN ABB. POST. 70% - MILANO

4ever

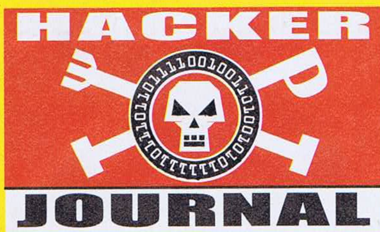
LINUX su XBOX

MINACCIA GIALLA
Il BOOM dei PIRATI in CINA

Anno 3 – N. 52
3 Giugno 2004 - 17 Giugno 2004

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."



editoriale

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Romina "Nikita" Grasselli, Luciana "Zingy" Mascolo, Cesare "Clark" Salgaro, Cristina "Caffeina" Morelli, Veronica "Pollon" D'Adda, Davide "Pupis" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

SIAE anche su Internet: è legge di Urbani

Dopo tanti strombazzamenti di modifiche da parte dei legislatori ed emendamenti annunciati da parte dell'opposizione, le prime sono state fatte solo in parte e i secondi sono stati ritirati. E il decreto Urbani è diventato legge italiana. Siamo il primo paese ad avere una legge così restrittiva e a favore dell'attuale e obsoleto sistema di distribuzione delle opere d'ingegno, di qualunque tipo. Il primo paese a non aver considerato il poderoso cambiamento che Internet ha prodotto nelle modalità di distribuzione di qualunque cosa. Hanno affermato che la legge verrà modificata – ed è già un paradosso approvare una legge riconosciuta zoppicante dagli stessi estensori - ma intanto l'hanno approvata. Hanno anche detto che è in fase di sperimentazione: ma intanto se i siti che distribuiscono qualunque opera dell'ingegno (e non solamente file musicali o video!) non si mettono in regola con i diritti d'autore – cioè non pagano la SIAE – incorrono in sanzioni.

L'uso personale ne esce quasi salvo, ovvero è riconosciuta la possibilità di copia ad uso esclusivamente personale e non a fini di lucro. C'è quindi da supporre che se scarichiamo file in misura moderata e a un ritmo tale che non faccia supporre l'uso a fini di lucro, siamo abbastanza protetti. Ma attenzione! Dall'altra parte, chi ci fornisce il file, ovvero chiunque immette in rete delle opere d'ingegno, dovrà corredare il sito di un avviso che affermi di avere assolto gli obblighi sul diritto d'autore, ovvero di avere pagato la SIAE: in caso contrario le pene vanno da 154 a 1.032 Euro se recidivi. Fino a sei anni di reclusione invece per chi fa commercio con attività illecite.

Ciliegina sulla torta: è stato introdotto un prelievo del 3% per i produttori, destinato alla SIAE, sul prezzo di listino dei masterizzatori. Se la quota non viene versata comporta una sanzione doppia, del 6%, per i produttori. I provider ne escono illesi: nessuno gli chiederà più nulla se non in caso di inchiesta giudiziaria, esattamente come prima.

Chi ci guadagna in tutto ciò (oltre la SIAE)? Certamente Cinecittà Holding SpA, che si è vista approvare all'interno dello stesso testo un contributo straordinario di 3 milioni e mezzo di Euro.

Urbani è soddisfatto. Gli utenti?

Ma attenzione! Un'altra assurdità ci aspetta dietro l'angolo: è stato approvato l'obbligo di depositare tutti i contenuti dei siti web in un apposito "registro", come già adesso avviene per le pubblicazioni periodiche cartacee.

Ne parleremo la prossima volta...

TheGuilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Brevetti anche in EUROPA

Minaccia per la libertà del software o regolamentazione necessaria? Per noi ci voleva più equilibrio su tutti e due i fronti

Il consiglio europeo dei ministri sulle competitività ha scavalcato il voto contrario dell'Europarlamento e ha deciso di rendere brevettabile il software, come già avviene negli Stati Uniti. Il rischio sta in una parola: furbizia. Supponiamo, infatti, che qualcuno decida di brevettare l'operazione logica XOR, oppure un concetto software come "usare istruzioni nulle per rallentare un processo". Cosa potrebbe accadere? Il 99% dei programmi creati, non potrebbe essere più commercializzato o dovrebbe pagare dei diritti ai detentori del brevetto.

Dette così, le cose portano a una visione assolutamente catastrofica. Perché chi si mette più a scrivere software, se per ogni riga di codice di routine assolutamente scontate sa di dover pagare diritti alle multinazionali di turno, le uniche con la potenza economica e legale per affrontare la brevettabilità?

E infatti a parole sono tutti contro.

Il Ministro dell'Innovazione italiano Lucio Stanca ha voluto diramare una nota affermando che la direttiva approvata è "contraria non solo agli interessi tipici italiani e delle piccole e medie imprese del settore informatico ma, in generale, crediamo che più si consente il ricorso al brevetto nel software e più si limita il suo sviluppo".

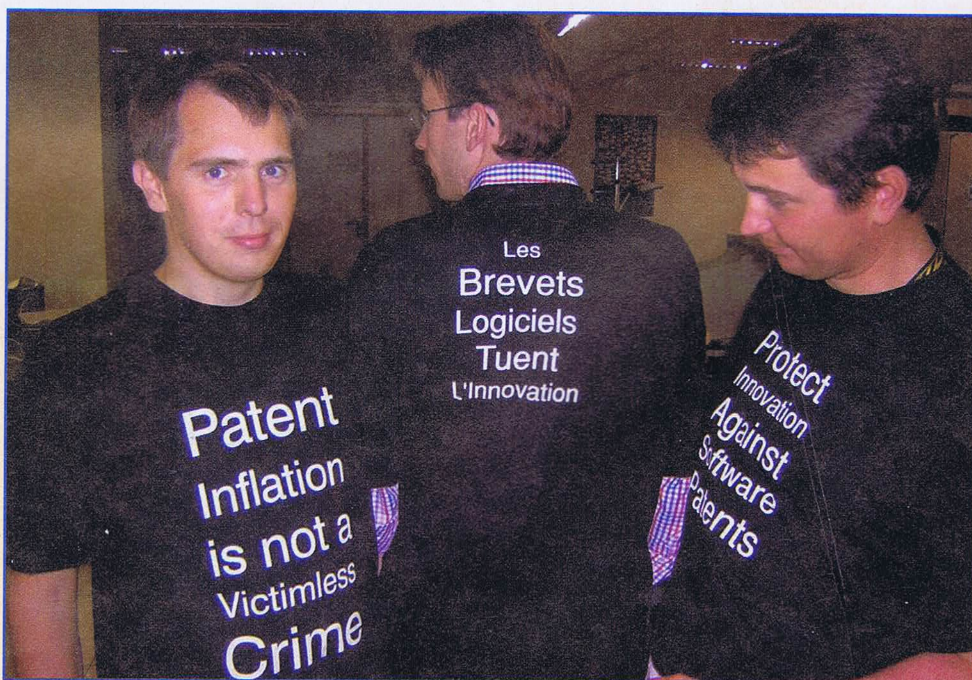
Giustamente, fa notare il ministro, la brevettabilità è un concetto che con il software si sposa malissimo. Perché da un lato è giusto proteggere soluzioni dell'ingegno di chi ha scritto software, ma dall'altro bisogna lasciare qualche tipo di libertà perché, altrimenti, si blocca tutto quello che oggi comporta l'uso di codice. Cioè tutto. Siamo circondati da software ovunque: da quando accendiamo una lampadina minimamente "intelligente" a quando facciamo funzionare il telecomando o andiamo in automobile. Quindi?

Quindi sarebbe meglio usare strumenti di legge alternativi, ma più deboli. Come far rispettare il copyright, che è una forma di riconoscimento di appartenenza, ma non è così restrittivo e pesantemente sanzionabile. E magari migliorarlo.

Dopodiché guardiamo agli altri Paesi. Gli esempi che abbiamo fatto all'inizio non li abbiamo inventati: negli Stati Uniti c'è chi ci ha brevettato esattamente quanto abbiamo detto e molto di più, come si può vedere a http://www.base.com/software-patents/examples.html.

Che cosa è accaduto? Che al momento sono il paese più progredito a livello tecnologico e software. Mah, i paradossi del sistema occidentale non finiscono mai di stupire. Prima di essere "contro" qualcosa, vale sempre la pena informarsi bene.



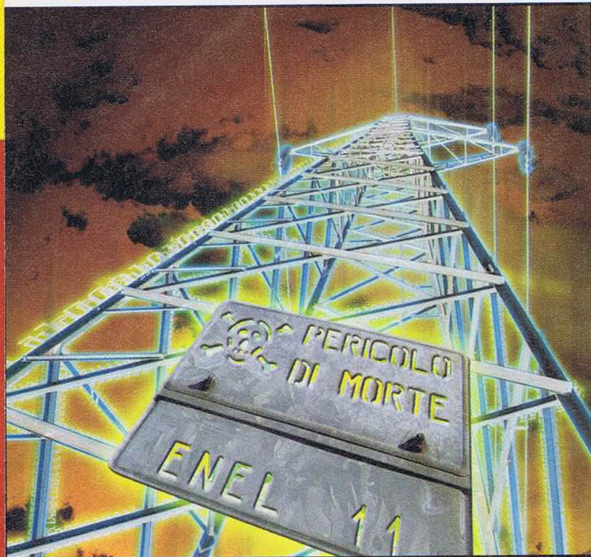


NUMERO 5.251.165

Generazione di numeri casuali mediante il passaggio dell'output di un generatore di numeri casuali come input di un altro generatore di numeri casuali.

Brevetto problematico per la libertà del software o solamente stupido e ignorabile? Non sempre è facile distinguere. L'Italia si è astenuta dal voto, pur essendo contraria, e forse sarebbe stato meglio un voto contrario, ma poteva andare peggio...

MA QUANTO MI CONSUMI?



Volevo farvi una piccola critica su un articolo pubblicato nel numero 48 pagina 30 sul consumo dell'energia elettrica del computer. Per vedere cosa effettivamente costa in un'ora voi avete detto di utilizzare la legge di Ohm,

*p(w)=v*i*

Ma questa formula funziona solo nei circuiti a corrente continua e non in quelli a corrente alternata. Per i circuiti in corrente alternata bisogna tenere conto della variabile j, l'angolo di sfasamento tra la tensione e la corrente, quindi la nuova formula sarà:

*P=V*I*cosj*

Quindi, per misurare la potenza reale in corrente alternata, sono necessari un voltmetro, un amperometro e un fasometro (che misura l'angolo di sfasatura) ed è poi necessario eseguire il prodotto delle tre grandezze misurate. Si verrebbe altrimenti a propagare un errore di misura pari alla somma degli errori relativi delle tre singole determinazioni. [complimenti]

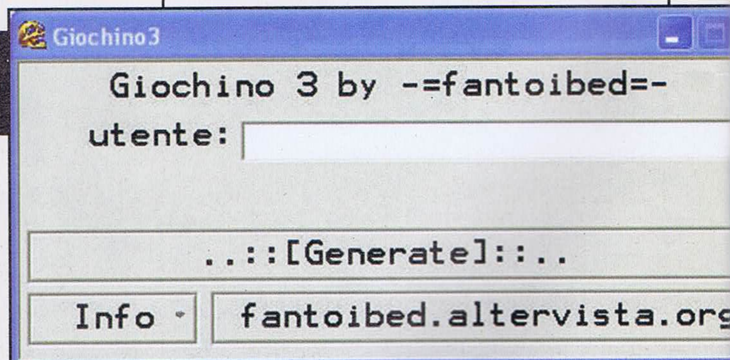
Davide

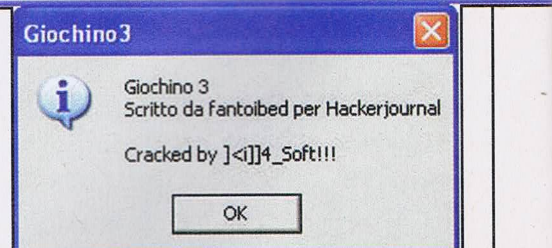
Bravissimo. Infatti nell'impaginazione dell'articolo, per problemi di spazio, è saltato un box che riportiamo qui:

DOVE STA IL DIFETTO

I più bravi ci smentiscono subito e hanno ragione. Infatti le misure che stiamo facendo tramite il nostro tester sono effettivamente fatte su una corrente che scorre nella resistenza, ma in alternata e con un carico non puramente resistivo, come vorrebbe la legge di Ohm. Cosa vuole dire? Il nostro PC non è sempre come una lampadina, che assorbe corrente senza influire in alcun modo sul 'come' questa si comporta nel circuito. Perché contiene anche degli avvolgimenti, dei condensatori e parecchi altri componenti che influiscono sul comportamento della corrente, istante per istante, dentro il nostro circuito.
Inoltre il tester che utilizziamo non è necessariamente il meglio in assoluto. Se non è capace di misurare il valore efficace, detto True RMS, i disturbi sulla forma dell'onda della nostra corrente alternata potrebbero falsare le misure. E allora? Allora spendiamo 39 Euro e acquistiamo un misuratore finito, oppure accontentiamoci, come abbiamo fatto noi, e usiamo il nostro sistema per paragonare tra loro diversi PC e capire, per confronto, con quale spendiamo meno nella bolletta dell'Enel.

IL GIOCHINO MODIFICATO. ECCO COME SI DIVENTA HACKER: UN PROGRESSO, ANCHE PICCOLO, ALLA VOLTA



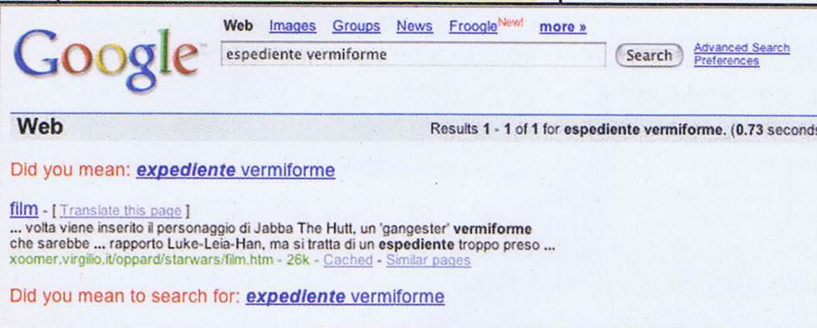


Ciao redazione di Hacker Journal, Mi chiamo Simone e ho 15 anni; Mi sono divertito molto a modificare il Giochino3.exe che avevate proposto su HJ n°48 in modo ulteriore a ciò che era stato proposto e guardate cos'è diventato!!! Praticamente un vero e proprio password generator ove si inserisce solo lo username e in cambio si riceve la password.
Siete mitici!
(Non è che sapreste consigliarmi un buon libro sull'assembler?)

]<i]]4_ximon

Ciao Simone!
Sei stato bravissimo e possiamo solo farti i complimenti. I libri in italiano sull'Assembler sono tutti vecchiotti, se stai considerando l'Assembler x86 (se desideri altri processori il linguaggio cambia). Puoi provare Il linguaggio di programmazione Assembler 8086/8088 di Prinetto-Rebaudengo-Sonza Reorda Matteo (sembra una canzone di Sanremo!), 285 pagine, 1996, 22,95 euro su http://www.gorilla.it. Se invece te la senti di affrontare l'inglese (molto meglio), cerca su Amazon.com e troverai più scelta. Se sei nella zona di Milano puoi trovare libri tecnici stranieri anche presso la libreria Hoepli, in via Hoepli.

GOOGLEWHACK, ANCORA PIÙ DIFFICILE



Due parole, un solo risultato. Ma chi riesce a trovare due parole che sono una vicino all'altra nella stessa pagina? Magari usando addirittura diversi motori di ricerca

Ciao,
vi mando in allegato alcuni googlewhack che ho trovato in una mezz'oretta di tempo libero. Ho anche una sfida da proporre: si tratta di trovare googlewhack di due parole consecutive (cioè tali che la pagina linkata le contenga una dopo l'altra). Io non ne ho ancora trovati.

pedissequi pedanti
palindromi gustosi
rivoluzioni onomatopeiche
costrizioni munifiche
molibdeno idilliaco
accumulatori culinari
ridicoli erbivendoli
apostata affabulatore

Vi mando alcuni miei googlewhack:

espediente vermiforme
pargolo piroettante
piretro cremisi
palazzine boliviane

Giuliano

Ricordiamo che un googlewhack consiste nel trovare due parole italiane che, cercate su Google in modo generico, risultano in una e una sola pagina Web. Ma la sfida che propone MB è ancora più difficile: nella pagina le parole devono apparire una accanto all'altra. Chi è così bravo da riuscirci?

RADIO AEROPLANO

Salve ragazzi sono un vostro assiduo lettore, ho letto con interesse l'articolo "Basta una radiolina" pubblicato nel numero 50 di HJ per captare le comunicazioni radio tra pilota e torre di controllo. La modifica da effettuare sulla radio è abbastanza semplice e in teoria dovrebbe funzionare. Mi sono però consultato con un radioamatore nonché esperto di tutto ciò che ha a che fare con l'etere. Per lui la modifica è fattibile, peccato però che questo tipo di comunicazioni radio avvenga in AM anziché in FM e pertanto mi dicono che la ricezione risulterebbe fortemente distorta e quindi ai limiti della comprensibilità. Ci potete chiarire come ci siete riusciti?
Inoltre avete scritto che la frequenza diminuisce al diminuire dell'induttanza (che a sua volta diminuisce al diminuire delle spire e aumentando lo spazio tra esse) poi invece nel riquadro celeste riportate che Diminuzione delle spire + Variazioni di spaziatura = INCREMENTO della frequenza (?) credo che la verità sia sul riquadro. Grazie, comunque continuate così.

Daniele Melis

Intanto possiamo confermare che le comunicazioni dell'aviazione civile avvengono in AM, però è anche vero che la FM delle radioline non è "a banda stretta" ma si parla di FMW (cioè FM a banda larga, con poca selettività di canale). Pertanto le comunicazioni risultano un po' "gracchianti" ma solo limitatamente, posso garantirti che la comprensibilità non è un problema. In merito al numero di spire, l'induttanza aumenta all'aumentare del numero delle spire e la frequenza diminuisce. Quindi per aumentare la frequenza occorre diminuire il numero delle spire. Probabilmente c'è stato un "lapsus". Confermo che per aumentare la frequenza occorre diminuire il numero di spire.

P. S. in alcuni casi la comunicazione può essere distorta, ma avviene solo se il segnale è molto forte (es. aereo a bassa quota sopra la nostra casa).



Va bene ascoltare gli aerei in volo, ma occhio alle induttanze!

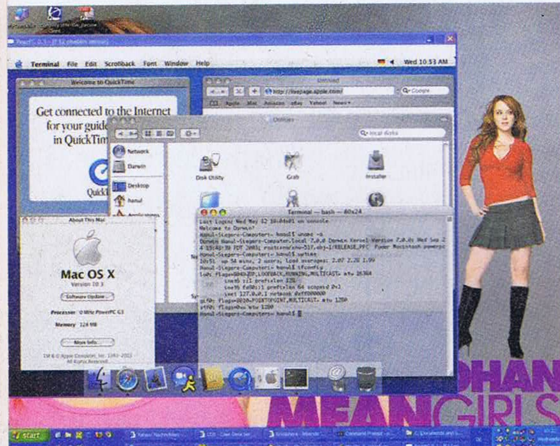
HOT!

METTI MACOS X SU WINDOWS

PearPC è un nuovissimo emulatore di un'architettura PowerPC, installabile (per ora con qualche complicazione) su piattaforme Windows.

È un software Open Source che sta muovendo i primi passi, sicuramente ancora da sviluppare e migliorare, giunto alla versione 0.1.1 e raggiungibile al sito http://pearpc.sourceforge.net/

Chi ha provato a installarlo per metterci sopra MacOSX 10.3 ha detto che è un'esperienza entusiasmante, seppure con le attuali limitazioni che lo rendono lento e ancora suscettibile di crash. È un prodotto ancora suscettibile di tante modifiche. Ma ha tutte le premesse per darci la possibilità di far girare i sistemi operativi ora proibiti su macchine.



SEMINARI GRATUITI SU LINUX E LATEX

Linkatevi all'indirizzo Internet https://www.universibo.unibo.it/. Nella sezione "Servizi" ci sono i rimandi a seminari su GNU-Linux e Latex.

I seminari sono gratuiti e aperti a tutti. Una lezione a settimana (sabato mattina Linux e mercoledì sera Latex). Si svolgono a Bologna presso la facoltà d'ingegneria in viale Risorgimento 2.

FALLIMENTO TOTALE!

Nel numero 47 di Hacker Journal avevamo dato la news della competizione tra veicoli autosufficienti, che dovevano attraversare un bel po' di chilometri di deserto e di territorio disabitato senza controllo umano. Era stata lanciata dal dipartimento della difesa americano e hanno partecipato decine di team, quasi tutti universitari, con i mezzi più assurdi. In palio un premio da 1 milione di dollari, che purtroppo non ha vinto nessuno. L Tutti hanno fallito per i motivi più diversi: chi per il sistema di posizionamento satellitare, chi per le caratteristiche meccaniche, chi per l'elettronica... comunque sia è stato bello e pare che l'anno prossimo la sfida si possa ripetere.



E volevano vincere con 'sto coso?

TCP VULNERABILE?

La "scoperta" è stata fatta da un ricercatore nello stato del Milwaukee, il quale è riuscito a bloccare una comunicazione TCP – sappiamo che praticamente tutte quelle che transitano su Internet sono tali – inviando un'opportuna sequenza di pacchetti TCP con settati i flag RST e SYN.

Se i router non sono sufficientemente attrezzati, possono quindi essere bloccati dalla sequenza opportuna inviata da parte di chiunque. Dove sta il problema, ci chiediamo? Sta nel fatto che, pare, praticamente tutti gli apparati presenti in rete, anche i più grandi e sulle vie di comunicazione più importanti, sono vulnerabili. Possibile? Si, a giudicare dall'importanza che viene data all'avvertimento da parte del National Infrastructure Security Co-ordination Centre (http://www.uniras.gov.uk/vuls/2004/236929/index.htm).

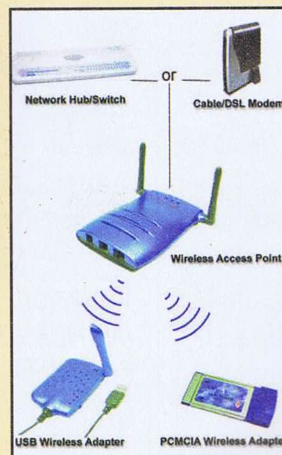


Dove, però, stanno apparendo anche le nuove versioni dei software che fanno funzionare i router delle principali società che li producono.

Ora, ci chiediamo, possibile che un protocollo conosciuto da vent'anni possa causare ancora inconvenienti di questo tipo? Morale: mai abbassare la guardia.

POSSIBILI ATTACCHI DOS SU WIFI

L'Australian Computer Emergency Response Team (AusCERT) ha emesso un comunicato di allarme denunciando il fatto che il protocollo 802.11b può essere sottoposto a attacchi DoS (Denial of Service). Il problema nasce da come i dispositivi 802.11 cercano di negoziare tra loro. Infatti i nodi di una rete WiFi usano il CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) per evitare di trasmettere contemporaneamente, tramite una procedura denominata Clear Channel Assessment (CCA). Chiunque potrebbe, con un qualsiasi terminale wireless, infilarsi nella procedura CCA e convincere tutti i terminali e gli Access Point che si trovano nel suo raggio d'azione che il canale è occupato. Tutti i dispositivi interessati smettono di trasmettere e la rete si blocca. Il problema riguarda tutti i protocolli 802.11 sotto i 20 Mbps, mentre non c'è pericolo per il nuovo 802.11a l'802.11g a 54 e 108 Mbps.



È IN EDICOLA IL SECONDO NUMERO!

Webmaster Journal è la rivista ideale per chi vuole creare un sito internet da zero e metterlo in rete senza fatica in pochissimo tempo. Che si tratti di fare un lavoro su commissione o di creare pagine Web per mostrare la nostra abilità, Webmaster Journal è lo strumento più semplice e immediato, perché tratta tutti i temi caldi di internet, dalla progettazione dei siti alla scelta degli strumenti e dei programmi per realizzare efficacemente i nostri progetti. Ogni pagina fornisce istruzioni che possono essere usate subito apportando delle semplici modifiche alle pagine che vengono incluse sul CD. Inoltre, nel CD di questo numero di Webmaster Journal si trova la versione completa della raccolta di programmi Acdsee 4.0 Powerpack. La raccolta, gratis per i lettori, comprende AcdSee 4.0, Foto Canvas e Foto Angelo: tre strumenti per trattare le immagini impareggiabili per potenza e semplicità d'uso. Sul CD si trovano anche programmi di grande utilità come EZTimeSync 3.7 o Antenna Web Design Studio, e strumenti di livello professionale come Flash MX 2004 e Fireworks MX 2004. Oltre ai consigli e alle guide pratiche che troviamo nelle pagine di Webmaster Journal, possiamo approfittare anche delle raccolte di modelli gratuiti per pagine web e sfruttare i moltissimi elementi già pronti che rendono più facile la vita di chi lavora con Internet. Infine, uno staff di esperti è a disposizione per risolvere i piccoli intoppi che ogni giorno si presentano al webmaster. Webmaster Journal è la rivista per chi vuole fare soldi e divertirsi con il Web.





HOT!

ANCHE A CISCO HANNO RUBATI I CODICI



800 Mb di codice, relativo all'ultima versione (la 12.3 e 12.3t) del sistema operativo degli apparati di rete Cisco, sono stati trafugati dalla rete interna all'azienda e in parte pubblicati su un sito russo.
La società ha confermato l'autenticità dei file contenenti il codice sorgente, ma non ha saputo dire se questi siano stati trafugati dopo una violazione della propria rete. Cisco sarebbe comunque più protetta rispetto a Microsoft, che aveva subito il trafugamento di parte del codice sorgente di Windows, per la natura stessa dei suoi apparecchi. Il codice Windows è infatti analizzabile su qualunque PC, mentre il codice di Cisco richiede hardware specializzato, per cui la compilazione del codice sorgente è molto più difficile.



MINACCIA GIALLA

"Questo è il nostro Paese. Questa è la nostra gente. Se non agiamo noi, chi agirà?". Questo slogan di Mao Zedong campeggia sulla home del sito degli Hongke, gli hacker più attivi della Cina, e riassume il loro credo di ribellione, politico e insieme nazionalista.

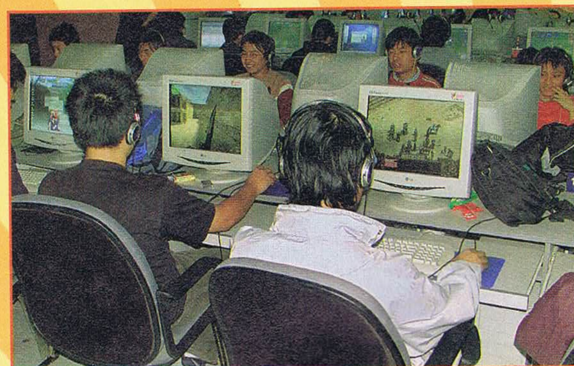
Per il governo sono nemici, ma dipende

Il governo cinese si è accorto con ritardo degli hacker di casa propria. È solo nel 2000 infatti che Xu Rongsheng, rappresentante della Cina presso l'UNESCO, ha ottenuto l'OK alla creazione della prima forza cinese antihacker che, forte di una dozzina di componenti, si propone di proteggere i siti governativi, specialmente quelli delle istituzioni finanziarie, dagli attacchi informatici. Il primo ad accorgersi dell'efficacia di queste misure è stato Wang Qun, studente originario del centro del Paese, che nel settembre 2001 è stato arrestato per il defacciamento di alcune pagine di siti ministeriali, sui quali aveva inserito immagini erotiche. Le autorità cinesi, peraltro, sono molto più compiacenti nei confronti dei defacciatori di siti americani e giapponesi, soprattutto nei momenti di maggiore tensione politica. Un esempio evidente è quello della Honkers Union of China (http://www.cnhonker.com/), gruppo di hacker estremamente politicizzato, che non ha subito conseguenze pur essendo responsabile di numerosi attacchi a siti esteri. La loro impunità lascia supporre che siano sostenuti in qualche modo dal governo cinese.



Apparsi a metà degli anni '90, i primi hacker della Cina soffrono di un notevole ritardo tecnologico rispetto ai colleghi americani o di casa nostra. I computer erano arretrati, l'accesso a Internet restava un lusso per privilegiati e i primi internauti si accontentavano di scambiarsi idee sui BBS, roba che noi facevamo dieci anni prima, ma che da loro è molto praticata tutt'oggi. Per un po' la pirateria ha riguardato esclusivamente la copia abusiva di software straniero. È la politica internazionale a portare alla ribalta gli hacker cinesi, quando – nel 1998 – si verificano tumulti xenofobi in Indonesia e tra le vittime vi sono anche cittadini cinesi, che vedono sequestrati i loro giornali e date alle fiamme le loro abitazioni. Se la maggior parte del popolo cinese provò una forte emozione ma altrettanta impotenza, la comunità hacker sentì l'impulso ad agire e fare qualcosa. Muniti di poca tecnologia e molta voglia di fare intasarono le caselle di posta elettronica del governo indonesiano. Fu, secondo le loro parole, la prima guerra cibernetica di difesa della Patria, che portò alla nascita di diverse organizzazioni all'interno della nazione cinese.

In cinese, hacker si dice "hei ke", letteralmente "passeggero nero", colore che in Cina simboleggia l'illegalità. Così i diversi movimenti hanno scelto di distinguersi attraverso i colori, lasciando vedere tre tendenze emergenti. Gli Hongke, molto politicizzati, sono i "passeggeri rossi": gruppo più influente del Paese, e quinto raggruppamento di hacker al mondo, sono all'origine delle cyberguerre e godono del tacito sostegno del governo.



维护中国网络安全的精锐之军

中国黑客第一军团



Hanno creato il loro sito all'indomani del bombardamento dell'ambasciata cinese a Belgrado nel 1999, con un grande successo e oltre 500 mila visite ricevute in pochi giorni. Nell'aprile 2001 hanno fatto partecipare 80 mila persone a un attacco di siti americani per protestare per la collisione tra un aereo cinese e un ricognitore statunitense. Per qualche giorno su numerosi siti istituzionali a stelle e strisce apparve il vessillo cinese, accompagnato da slogan come preserviamo la sovranità nazionale, disonore a chi non resiste o attacchiamo l'arroganza anticinese.

Sono più pacifisti i Lanke, "passeggeri blu", focalizzati sulle questioni tecnologiche e i problemi della sicurezza sulla Rete. Anche più attenti alle logiche del capitale: nel luglio 1999 i cinque fondatori hanno infatti fondato un'impresa specializzata in sicurezza informatica, dove oggi lavorano una sessantina di dipendenti.

Dopo le cyberguerre il gap tecnologico degli hacker cinesi si è ridotto. Nel 1998 nasceva il loro primo trojan, Netspy. E infatti nell'ottobre 2000 una azienda di Canton ha creato un firewall, Blue Shield, riconosciuto dal Ministero della pubblica sicurezza come il primo prodotto di difesa interamente cinese. Un'altra azienda ha messo in commercio nello stesso periodo il programma "hacker killer", capace di combattere oltre 800 metodi di pirataggio informatico. "Gli hacker – ha affermato un dirigente – hanno contribuito alla ricerca cinese, evidenziando problemi di difesa e inventando software per la sicurezza". Militanti politici nazionalisti o piccoli geni della tecnologia, gli hacker cinesi mirano comunque a conservare una loro indipendenza dalle autorità locali e mantenere un atteggiamento vagamente romantico, come dimostra un passo preso dalla rivista Hacker X Files: "In effetti anche uno psichiatra è un hacker, uno di quelli che penetra nei cervelli. Ma noi, noi salviamo la gente…".



Internet e/o libertà

Nelle mani dei governanti cinesi Internet può essere uno strumento a doppio taglio. I 470 mila siti del Paese più popoloso del mondo offrono agli internauti una grande finestra sul mondo, che minaccia in continuazione il drastico controllo informativo esercitato dallo Stato sugli altri media. Ma i 70 milioni di internauti cinesi, l'80 percento dei quali ha meno di 24 anni, devono stare attenti a maneggiare l'apparente libertà del loro Web: secondo uno studio di Reporter senza frontiere, pubblicato nel giugno 2003, la Cina detiene il triste record dei cyberdissidenti imprigionati, con 42 persone condannate a pene da 3 a 15 anni di reclusione per la pubblicazione su Internet di informazioni contrarie agli interessi governativi.

Il governo cinese mantiene una stretta di ferro su Internet. Per esempio è impossibile, da dentro la Cina, accedere alle pagine web di Amnesty International o dei tibetani che lottano contro un'occupazione militare che dura da decenni. Ma Mao stesso osserverebbe che, a stringere troppo il pugno, la sabbia sfugge tra le dita…

S. Bardon





Colpo basso a

Ecco come possiamo installare Linux sulla nostra XBox per smanettare e, nel tempo libero, giocare



Questo è il metodo che ci porterà ad avere Linux sulla consolle XBox e allo stesso tempo potremo continuare a usarla per giocare.
Per prima cosa bisogna avere l'exploit giusto... quale? Esistono infatti due versioni diverse dell'exploit, che differiscono dalla presenza sulla consolle del servizio XBox-live.
Se è presente tale servizio, questo verrà sostituito da Linux mentre se non è presente verrà creata l'opzione nel menu che ci darà la possibilità di avviare il nostro sistema operativo preferito.

Tramite il software gestionale dell'action replay salviamo l'exploit nella

ABBIAMO BISOGNO DI:

- una XBox mai modificata
- una copia del gioco MmechAssault (vari giochi XBox permettono di far scattare i bug che affliggono la consolle... poverina)
- una memory card
- un PC con scheda di rete
- un modo per trasferire dati dal PC alla memory card oppure un pen drive

la distro Ed's debian

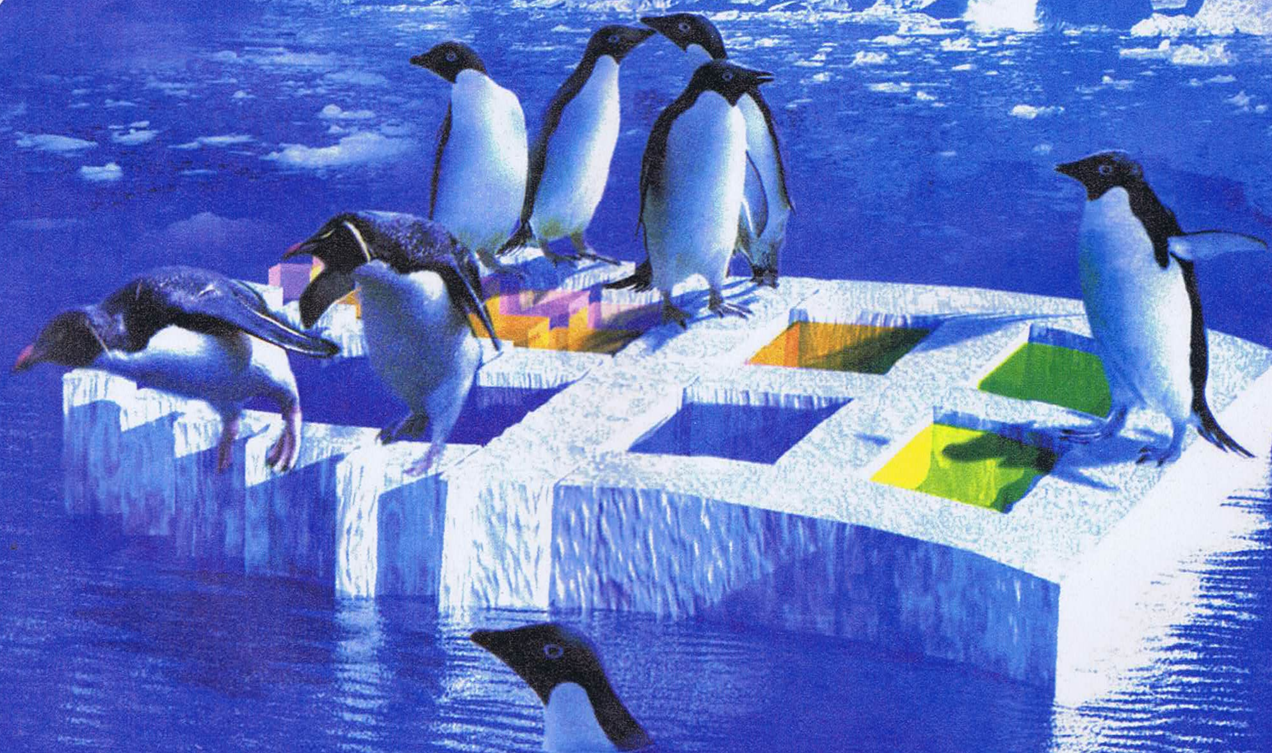
Innanzitutto individuiamo di quali componenti è composta la consolle:

Processore:	733 Mhz
Processore Grafico	NV20a 233Mhz progettato e realizzato da Microsoft e nVidia, 64 MB Memoria RAM
RAM	64 MB
Velocità di trasferimento memoria (Memory Bandwidth)	6,4 GB/s
Numero di poligoni (Polygon Performance)	125 M/s
Textures simultanee	4
Pixel Fill Rate (senza textures)	4.0 G/sec.
Pixel Fill Rate (1 texture)	4.0 G/sec.
Pixel Fill Rate (2 texture)	4.8 G/sec.
Texture Compresse	Si (6:1)
Utilità di memorizzazione	5x DVD, Hard Disk 8Gb (western digital) - 10Gb (Seagate), Memory Card 8Mb (accessorio)
Porte I/O	4 Porte Controller (USB), 1 Ethernet (10/100Mbps)
Canali Audio	256
Supporto Audio 3D	Si (64 Canali 3D)
Supporto Hardware MIDI/DLS2	Si
Filtro Audio Hardware ed equalizzatore	Si
Supporto Film DVD	DVD Kit necessario
Modem	No
Broadband	Si
Supporto Film HDTV	Si
Supporto Giochi HDTV	si
Antialiasing	si (hardware)
Risoluzione Massima	1920 x 1080
Risoluzione Massima	(2x32bpp frame buffers +Z) 1920 x 1080

Microsoft: Linux su XBox

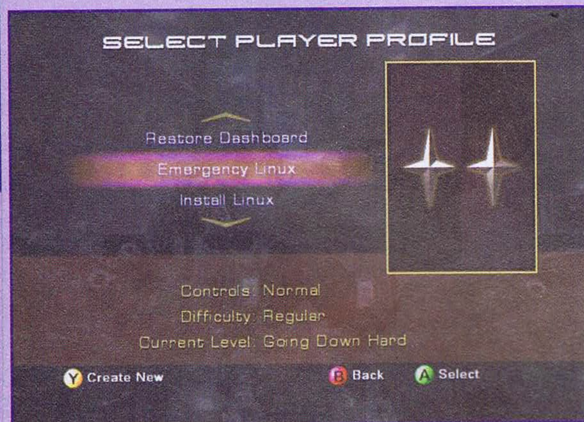
ATTENZIONE RISCHIO ROTTURA

Ovviamente non ci si assume nessuna responsabilità circa il successivo funzionamento della XBox dopo averla maneggiata in questo modo. Nessuno vorrà più ripararvi nulla se qualcosa andasse storto, a maggior ragione se la consolle è ancora in garanzia. Chi procede in queste modifiche lo fa a proprio rischio e pericolo (ma altrimenti, che gusto ci sarebbe?...)

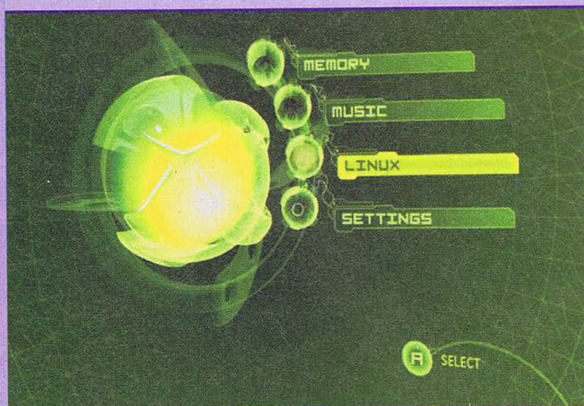




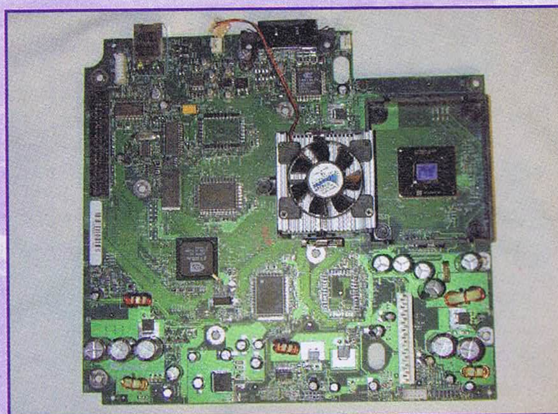
memory card: il salvataggio è di 2 Mb ed è diviso in 3 blocchi.
Dopodiché inseriamo la memory card nella console e spostiamo il savegame dalla memory card all'hard-disk del gioiellino Microsoft.
Ora abbiamo bisogno di una copia del bel gioco mmechAssault: avviamolo normalmente e nel menu Campagne ci saranno i 3 salvataggi spostati sull'hard-disk in precedenza. Selezioniamone 1:
1)restore dashboard, ci permetterà di re-installare la dashboard originale;



La videata dei salvataggi



Tutto quello che si desidera da una XBox



Piastra madre: meglio lasciarla dov'è.

2)install Linux, ci permetterà di installare una mini-distribuzione di Linux;
3)emergency Linux, ci permetterà di avviare una mini-ditribuzione di Linux.

Però non affrettiamo le cose. Alcuni pensano che convenga installare subito Linux, ma secondo noi è meglio fare avviare subito la mini-distro. Quindi carichiamo il salvataggio emergency Linux e, dopo averlo avviato, colleghiamo con un cavo il pc e la console.
Avviamo telnet e colleghiamoci all'IP 192.168.0.3, user:root, password: XBox. Digitiamo XBox_tool -a e premiamo invio: ci troveremo stampate a video tutte le informazione della console. Salviamole.

Ora riavviamo la console, carichiamo il gioco, ma questa volta carichiamo il salvataggio "install Linux" e seguiamo le istruzioni del video. Dopodiché spegnamo la console e teniamola spenta per una decina di secondi.
Naturalmente non possiamo usare Linux tramite joypad, ma bisogna avere un adattatore che trasformi la porta standard della console in una porta USB. Non vogliamo aprire la console, giusto? Quindi non vogliamo sostituire la porta del joypad della consolle (quella interna). Allora basta crearsi o acquistare il cavo. Noi consigliamo di autocostruirselo e dato che i cavi del joypad sono come quelli USB, basta congiungere i cavi con i rispettivi colori e il gioco è fatto; in questo modo possiamo collegare mouse e tastiera. La mini-distro è un po' scarna? Scarichiamo la distro Ed's Debian (l'unica compatibile), masterizziamola su Cd-Rw e inseriamola nella console: MechInstaller la avvierà.

Con questa procedura possiamo scegliere se giocare inserendo il gioco normalmente, vedere i DVD inserendoli a dashboard caricata, acoltare i CD audio normalmente oppure, selezionando la voce dal menu, avviare Linux. Questo metodo non ci permetterà di eseguire giochi backup, ma solo di avviare Linux dal menu. Se abbiamo dubbi oppure vogliamo chiarimenti, facciamoci sentire via email o sul forum!

Gennaro "BritHackEnza" Franzese
thx Phj&Candies crew
brithack@libero.it

LINK

http://XBox.manenti.org/
tutorial metodo software in italiano

http://www.XBox-tribe.com/
tutorial, download e tutto per la console, in italiano

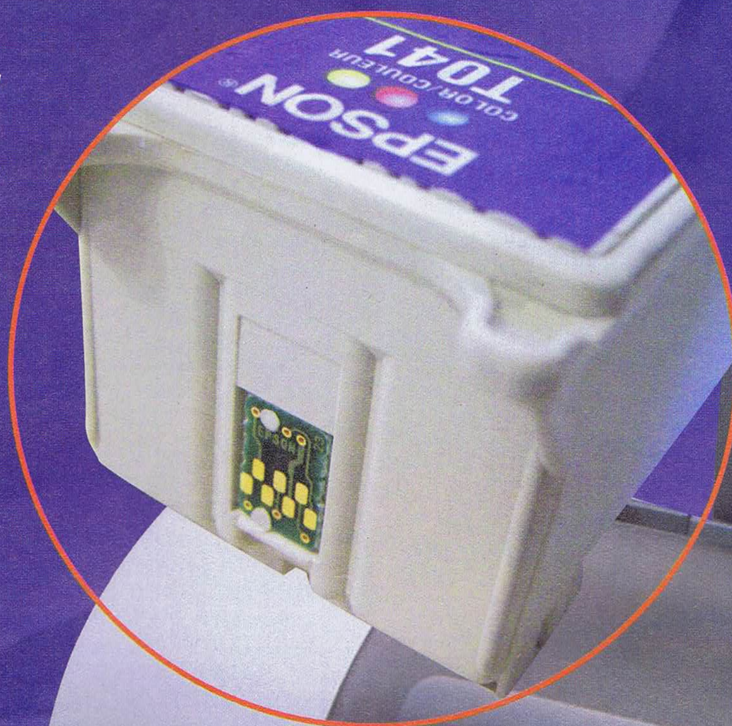
http://XBox-linux.sourceforge.net
tutto per installare Linux su XBox, in inglese

http://www.XBox-scene.com/
una vera miniera di informazione, in inglese

Basta!

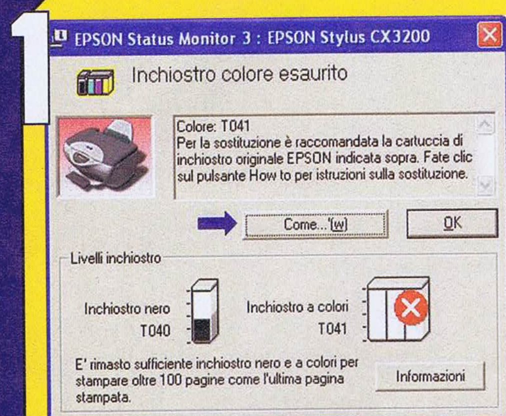
Siamo stufi di PAGARE EPSON!

Gli scandalosi prezzi delle cartucce "intelligenti" per le stampanti ink-jet ci svuotano il portafoglio. Vediamo come risparmiare aggirando i circuiti di controllo.



È già qualche anno che le cartucce per le stampanti ink-jet, di qualunque marca, costano a volte assai di più della stampante stessa. Siamo arrivati a vedere incredibili offerte di stampanti ink-jet a poco meno di 20 Euro, quando le cartucce di ricambio costano quasi il doppio. Ma c'è di peggio da quando sono nate le cartucce cosiddette "intelligenti": Epson insegna. I recenti modelli di stampanti Epson integrano, infatti, un chip che viene venduto come un sistema perfetto per tenere sotto controllo il livello dell'inchiostro, ma in realtà è solamente un sistema perfetto per costringerci a buttare la cartuccia quando il chip ci segnala la fine, perché senza l'ok del circuito la stampante si blocca.

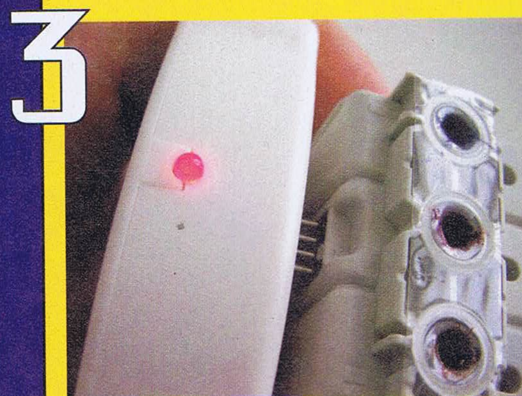
COME SI FA



Il chip ci segnala inesorabilmente che la cartuccia colore è esaurita. Sarà vero?



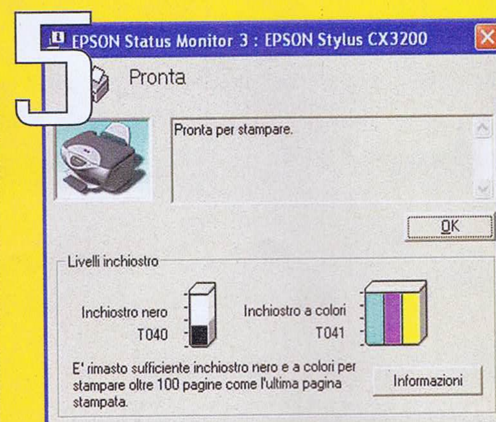
Estraiamola e guardiamo dov'è posizionato il piccolo circuito stampato contenente il chip che tiene conto del lavoro fatto dalla cartuccia.



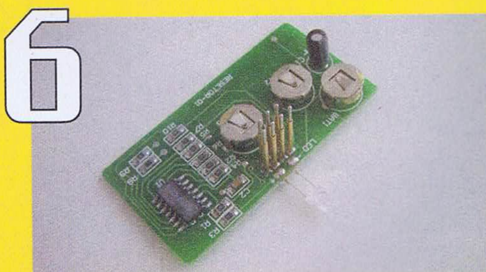
Appoggiamo con precisione i piedini che fuoriescono dal circuito del resetter ai contatti dorati del chip sulla cartuccia.
Il LED lampeggia.



Manteniamo qualche secondo il resetter appoggiato ai contatti, fino a che il LED diventa verde fisso.



Rimettiamo la cartuccia dentro la stampante e verifichiamone il funzionamento tramite il normale software installato sul pc. Perfetta: sembra che l'inchiostro non sia mai esaurito. Possiamo andare avanti a stampare ancora un po'. Se invece la cartuccia è veramente senza inchiostro, niente di più semplice che ricaricarla con gli appositi kit acquistati a basso prezzo.



All'interno del resetter un solo chip, due piccoli condensatori e qualche resistenza a montaggio superficiale. Un LED e i contatti per collegarsi al chip della cartuccia.

Intelligenti, ma non così tanto

Naturalmente non vale ricaricare la cartuccia con uno dei tanti sistemi già disponibili per inserire dell'inchiostro nei serbatoi, perché in realtà il chip non controlla per niente l'effettiva quantità d'inchiostro rimasta, ma solamente conta quante volte la cartuccia ha funzionato, così da calcolare approssimativamente la possibile rimanenza degli inchiostri.

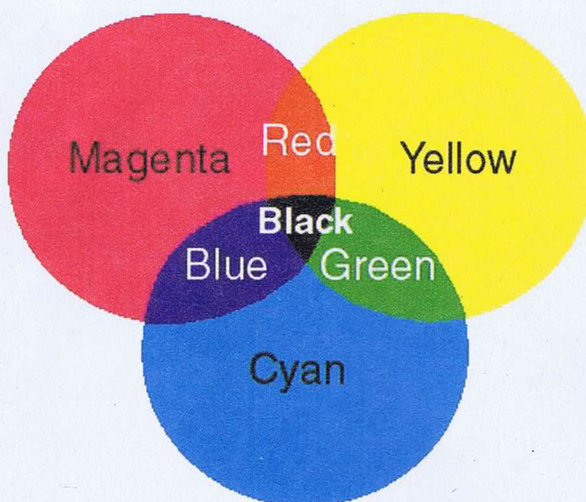
Finalmente un rimedio

Con 15,90 Euro ci dobbiamo procurare (www.qb7.com, ma in Italia per esempio presso www.tecnitron.it) un geniale apparecchietto che altro non è che un circuito integrato programmato apposta per resettare i circuiti dei chip delle cartucce Epson, riportando il valore interno esattamente allo stato iniziale, come quando la cartuccia è stata acquistata. Otteniamo così due vantaggi: sfruttare al massimo la cartuccia, esaurendo veramente tutto l'inchiostro contenuto anche dopo che il chip originale ha bloccato tutto per 'presunta fine dell'inchiostro'.
Poi ricaricare la cartuccia con i metodi di ricarica tradizionali,



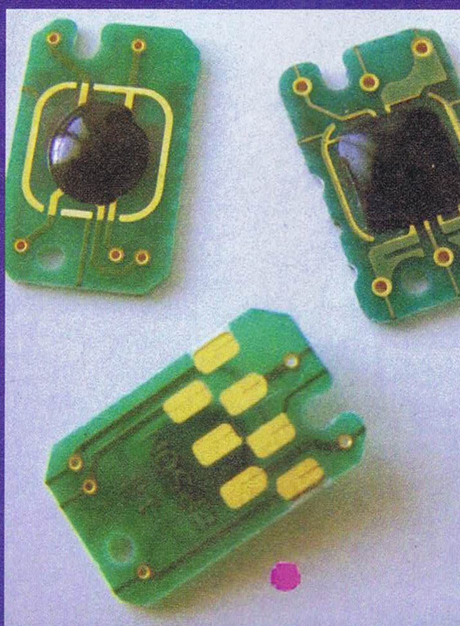
I colori fondamentali

Cyan, Magenta, Yellow: sono i tre colori degli inchiostri presenti nelle normali cartucce colore delle stampanti. Loro tre e il nero permettono di riprodurre qualunque altra gradazione di colore. In pratica corrispondono a una specifica tonalità di blu, rosso e giallo e dobbiamo stare molto attenti a inserire ciascuno dei tre colori nella sua giusta posizione all'interno della cartuccia che stiamo ricaricando.



"per risparmiare basta un apparecchietto da 15,90 Euro che possiamo comprare su www.tecnitron.it"

molto economici, ripristinando il contatore come se nulla fosse successo e quindi andando avanti a stampare come se la cartuccia fosse nuova.
Il tutto ripetibile, in teoria all'infinito. Nella pratica dopo tre-quattro ricariche gli ugelli della cartuccia potrebbero risentire di un po' di sporcizia e quindi stampare in modo meno preciso.
Comunque rimane un bel risparmio, anche perché le ricariche, che durano appunto per tre-quattro volte, costano quasi la metà di una cartuccia originale e funzionano comunque abbastanza bene!



Qualche chip Epson che, in teoria, dovrebbe impedirci di ricaricare le cartucce che lo montano.

I POSSIBILI PROBLEMI

• 1. Dopo che il LED rosso ha lampeggiato, non diventa verde:

- I contatti non sono ben posizionati o sono sporchi.
- Se la cartuccia non è originale Epson, potrebbe non essere compatibile con il resetter (ma in genere lo è).

Vale comunque la pena provare la cartuccia montata sulla stampante, perché il chip potrebbe essersi resettato ugualmente.

• 2. La qualità della stampa è decisamente scarsa

- Per la ricarica è stato utilizzato dell'inchiostro scadente. Oppure stiamo cercando di forzare la carica residua, mentre uno dei tre colori era realmente finito del tutto.
- Ci sono bolle d'aria intrappolate nella cartuccia, perché l'abbiamo ricaricata troppo velocemente. L'inchiostro va siringato nella cartuccia veramente molto lentamente. Si può anche provare a lasciare la cartuccia con gli ugelli verso il basso e ferma per almeno 24 ore (l'aria delle bolle sale ed esce dalle prese d'aria in alto).



L'HACKER,

Il trono di Re dell'hacking spetta a Kevin Mitnick, ma il posto di vice è occupato da Kevin Poulsen.

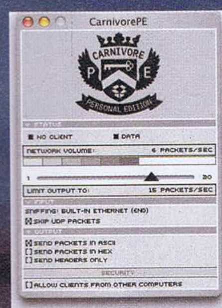
Nel 1965 a Pasadena, nella famiglia Poulsen si tirava avanti giorno dopo giorno con poco denaro ma molta buona volontà. Ed è lì che nasce Kevin. Da subito molti intravedono in lui delle doti particolari, soprattutto per quanto riguarda il mondo della tecnologia. A 17 anni Kevin riceve il suo primo computer: si tratta di un Radio Shack TRS-80 con il quale apprende la programmazione e, in modo specifico, può collegare a essa la sua già avviata attività di phreaking. È un successone, perché Dark Dante (questo il nome di battaglia) si dimostra abilissimo nell'utilizzo di tecniche di social engineering. Chi lo aiuta in questo hobby è Ron Austin, un grande amico, forse l'unico grande amico. Insieme progettano alcuni exlpoit che hanno come bersaglio l'Università della California e addirittura il Pentagono.
L'FBI se ne accorse , ma potè incriminare soltanto Austin, in quanto Kevin era ancora minorenne.



▲ *TRS-80: l'inizio della carriera*

La carriera segreta

Tale exploit verso il sito della difesa americana viene mitizzato dai giornali locali tanto che, una volta diplomatosi e passata la bufera, Kevin riceve immediatamente un'offerta di lavoro da un'importante società di software di Menlo Park. Il nostro ha così una scrivania legale come esperto di sicurezza informatica, ma nemmeno da lì rinuncia a pratiche di hacking… forte. Un bel giorno riesce a intercettare le telefonate dell'FBI e soprattutto a visionare archivi segreti dai server più importanti a livello istituzionale. Smaschera così operazioni di spionaggio dell'FBI stesso ai danni delle sedi diplomatiche quali Cina, Israele, India e Filippine. Accanto all'hacking forte, Dark Dante si diverte a scoprire numeri di telefono e incontri d'affari delle attrici da lui ammirate: Ally Sheedy ("War Game"), Molly Ringwald ("Breakfast Club"); nonché a presentarsi di persona a colloqui di lavoro: rimarrà famoso il caso di Madonna che oltre a Sean Penn si trovò di fronte proprio il nostro Kevin. Questa sua seconda attività verrà presto scoperta: oltre al licenziamento arriva anche l'arresto. La carriera è così compromessa? Nemmeno per idea. Kevin si rimette in moto. Il tribunale di San Francisco ha in mano documenti scottanti che potrebbero incriminarlo per vent'anni. Viene infatti perquisito un armadietto di Menlo Park, registrato sotto falso nome, dove vengono sottratti stampati top secret che confermano la sua attività di hacking definito "istituzionale" per il semplice motivo che proprio sedi istituzionali americane fungevano da obiettivo. Nel novembre 1988 inizia ufficialmente la latitanza di Dark Dante. Ciò che circolerà nei giornali sarà sempre e solo il suo nick.



Il client Carnivore in versione "personal"

La Porsche

Durante i diciassette mesi da primula rossa, Dark Dante riesce a mettere a

LA LEGGE, LA PORSCHE

segno gli exploit considerati più belli e affascinanti. Giugno 1990: una radio locale di Los Angeles, dove Kevin è nascosto, organizza un concorso radiofonico con in palio una stupenda Porsche 944 rossa fiammante. Scatta la gara. Kevin riesce a prendere il totale controllo delle linee telefoniche e a gestirne il flusso in entrata. Chi riusciva a fare la 102esima telefonata si aggiudicava la Porsche. Proviamo a indovinare chi alza la cornetta per quella telefonata?...
Il nostro, due mesi prima, aveva già vinto circa 10mila dollari adottando lo stesso metodo di attacco. Vinta l'automobile, Kevin la utilizzò sfrenatamente guidando con documenti falsi. Ed è a questo punto che l'FBI decide di "allargare" il caso a livello federale. I telegiornali parlano delle sue attività informatiche e trasmettono pure la sua fotografia. Un giorno dell'aprile 1991 Kevin si fa fregare nel modo più banale: sta facendo la spesa in un supermercato della California quando la cassiera riconosce il suo volto e avverte l'FBI. Kevin è già sulla strada verso casa e non ha il tempo di scappare: viene arrestato.

La condanna

Nell'aprile del 1995 ciò che il tribunale emette è una sentenza che farà storia: 51 mesi di reclusione, la bellezza di oltre quattro anni, 54mila dollari per l'exploit della Porsche e l'interdizione all'uso di computer fino alla fine del 1998. I capi di imputazione sono in totale 19 tra cui spiccano la frode informatica, la cospirazione, l'abuso di intercettazioni telefoniche e il riciclaggio di denaro.
La vita per Kevin ricomincia così il 4 giugno del 1996. Nonostante l'interdizione e con la complicità di alcune indulgenze, trova ancora un lavoro presso una società di software.

È indubbiamente trasformato dall'esperienza: nato phreacker poi passato all'hacking spinto, Kevin Poulsen ha dato sfogo alle sue eccezionali doti, ma con quella superbia di troppo che l'ha condotto in galera. La sua vicenda ricorda molto quella dell'omonimo e ben più famoso Kevin Mitnick. I due, tra l'altro, sono stati i protagonisti della scoperta di SAS, un sistema (attualmente ancora in uso dalle agenzie di sicurezza americane con il nome di DCS1000 o "Carnivore") per intercettare abusivamente le chiamate dell'FBI. Una tecnica risultata utile a entrambi per sfuggire ai blitz indirizzati contro loro stessi. Indubbiamente una figura più legata allo spionaggio tecnologico che alle semplici passioni di ragazzo, ma forse per questo considerata più affascinante.
Oggi è un affermato giornalista on-line: autorevoli le sue collaborazioni con riviste del calibro di Wired, ZdNet e del sito specializzato in sicurezza informatica Security Focus.

I PROTAGONISTI

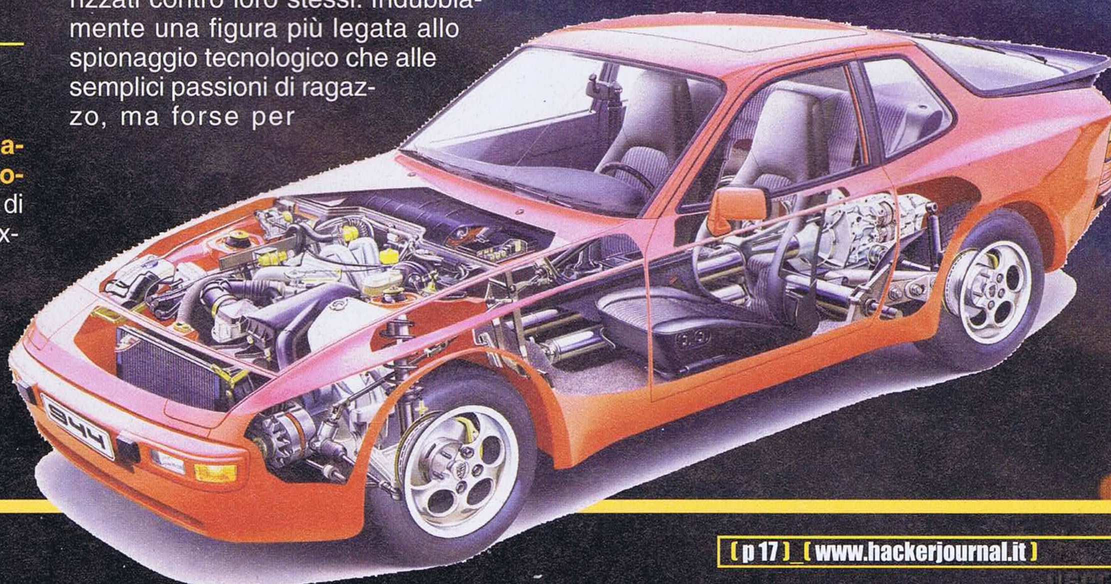


Kevin Poulsen in persona: schedato dall'FBI



Thomas Pickard: direttore dell'FBI

Alone Sparrow
kikocorsentino@email.it



Una Porsche rossa: l'inizio dei veri guai

TRUCCHI in rete: le

Qualche idea per newbie: cosa sono, come si utilizzano e dove si possono trovare in Rete le risorse per individuare i numeri IP e molto altro...

I modi che possiamo usare per effettuare una network query sono molti, ma si basano tutti sugli stessi comandi: in pratica si tratta di semplici utility che si possono lanciare da una finestra DOS o da un sito Web allestito con una specifica applicazione. Parecchie informazioni sull'appartenenza degli indirizzi IP già si trovano all'URL www.internic.net, ma noi vogliamo approfondire qualche tecnica in più.
Se vogliamo rintracciare l'origine di un IP o vogliamo sapere, di un host, a quale provider si appoggia per connettersi, possiamo compiere una particolare ricerca in Rete che sfrutta i Domain Name Service (DNS), che sono i software di Rete che associano a ogni IP il proprio host name e viceversa. In sostanza per collegarci a Internet noi scriviamo un host name, ma il programma comprende solo l'indirizzo IP, che è ciò che viene fornito dalla traduzione del DNS. Per ottenere informazioni da un DNS, basta lanciare da un sito di network query o semplicemente da linea di comando di una finestra DOS il comando nslookup: con il numero dell'IP otterremo l'host name e con l'host name otterremo il numero IP.

Dopo essere entrati in modo nslookup, possiamo anche lanciare il comando:

set type = <ANY>

che elenca tutte le risorse di un dominio, come server e-mail, name server ed eventuali altre, mentre se ci interessa proprio una specifica risorsa, possiamo digitare il suo nome al posto di ANY.

FINGER, PING, TIME

Finger funziona con alcune differenze sui sistemi operativi Windows e Unix e ricava informazioni private dal profilo dell'utente. Ping è invece un comando DOS che invia una richiesta di eco a un indirizzo IP o a un host, per verificare se esso esista veramente in Rete e se c'è stato scambio di dati.

La sintassi è:

-| ping host name
-| ping www.nomesito.com
-| ping xxx.xxx.xxx.xxx

Poiché il Ping è in realtà un (moderato) attacco flood, si deve prendere in considerazione che rallenta non solo il sistema da cui viene lanciato, ma soprattutto il sistema obiettivo e che quindi, se ripetuto, viene spesso inteso come tentativo di attacco e quindi tracciato.

Il comando Time interroga invece un remote host per ottenere il fuso orario, ed è molto utile quando si ha la necessità di verificare la collocazione geografica effettiva di un server.

TRACERT (TRACEROUTE)

Tracert è un comando DOS che visualizza il percorso compiuto in Rete dai pacchetti di dati, dall'host che ci interessa fino al nostro computer, indicandone i passaggi (salti o hop, cioè i vari

```
MySQL and Server Apache Manager :O)
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Ciao Standard :>

C:\Documents and Settings\Standard>tracert www.hackerjournal.it

Rilevazione instradamento verso www.hackerjournal.it [212.66.104.65]
su un massimo di 30 punti di passaggio:

  1   233 ms   236 ms   238 ms  lo1-3-3.dialup.edisontel.com [62.94.130.1]
  2   274 ms   219 ms   218 ms  g2-0.pd14.ec.edisontel.net [62.94.128.7]
  3   249 ms   162 ms   164 ms  a1-0-10.mi6.eb.edisontel.net [62.94.118.58]
  4   193 ms   155 ms   232 ms  infostrada-mix.mix-it.net [217.29.66.9]
  5   248 ms   172 ms   155 ms  151.6.0.53
  6   146 ms   225 ms   146 ms  151.6.0.62
  7   184 ms   151 ms   154 ms  151.6.33.218
  8   198 ms   202 ms   177 ms  gw-wind-s1-0.ltn.panservice.it [212.66.100.193]
  9   205 ms   169 ms   218 ms  fw-fas3-u.ltn.panservice.it [212.66.96.112]
 10   259 ms   184 ms   190 ms  server.hackerjournal.it [212.66.104.65]

Rilevazione completata.

C:\Documents and Settings\Standard>_
```

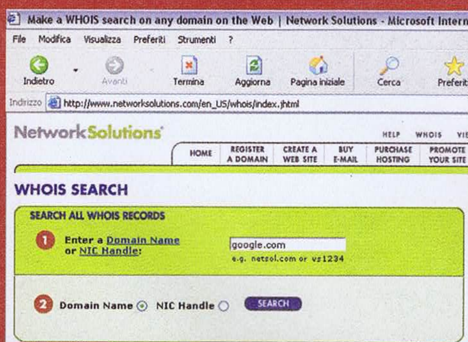
NETWORK QUERY

servizi che hanno fatto da ponte).
Tracert funziona inviando all'indirizzo IP oppure all'host che vogliamo rintracciare un pacchetto eco con valore TTL (Time To Live) uguale a 1: verrà respinto dal primo router, di cui verremo a conoscenza dell'IP, e ciò si verificherà con tutti i router successivi fino all'arrivo del pacchetto.

WHOIS

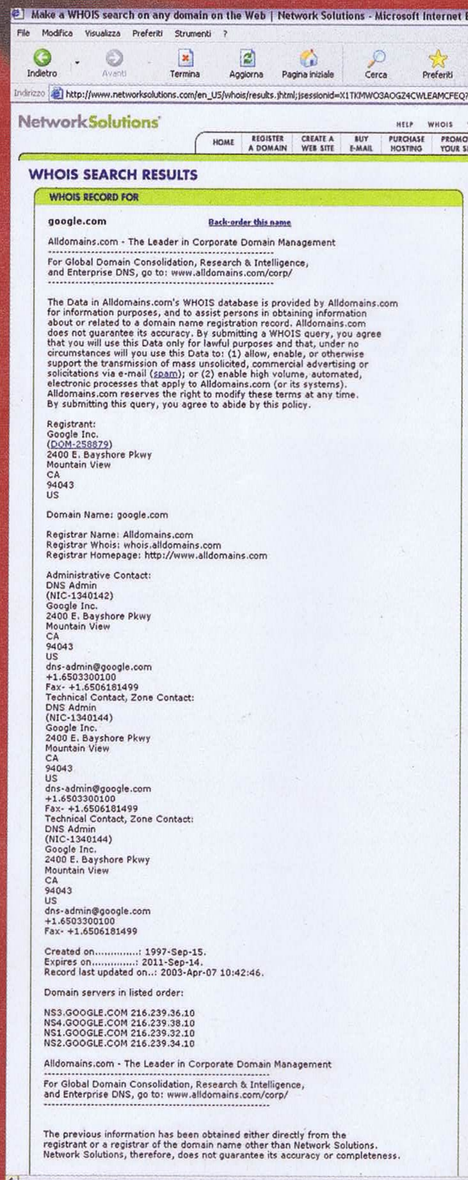
Il comando Whois ci permette di compiere una ricerca su un server WHOIS, digitando un dato qualsiasi, come un nome, un dominio, un host name e un indirizzo IP.

Siccome si rivela di grande utilità perché ci permette di ottenere molte informazioni (per esempio di un dominio), ecco qualche informazione in più.



WHOIS a Google.com

Supponiamo di avere la necessità di venire a conoscenza di informazioni riguardanti Google.com: ovvero dov'è la sua posizione geografica, il suo indirizzo e magari anche i numeri di telefono e di fax per contattare l'Amministrazione e i Tecnici. Il comando WHOIS potrebbe



essere una valida risposta.
Proviamo una ricerca su Google di siti da cui lanciare whois e troviamo un sito in inglese di nome NetworkSolutions.com. Google non solo ci ha trovato un valido sito, ma ci ha anche linkato sulla pagina che ci serve, evitando lunghe e noiose ricerche a partire dalla home.
Da qui inseriamo Google.com e proseguiamo con i passaggi suggeriti.

Al termine arriviamo su una pagina che ci informa su tutto (o quasi) ciò che riguarda il nostro obiettivo, il target finale. Adesso siamo un passo avanti per ottenere ciò che vogliamo.

Sono comunque tutti comandi da usare con la dovuta moderazione, perché impiegano risorse di rete e a volte vengono interpretati facilmente come tentativi di attacco da parte di chi stiamo testando.

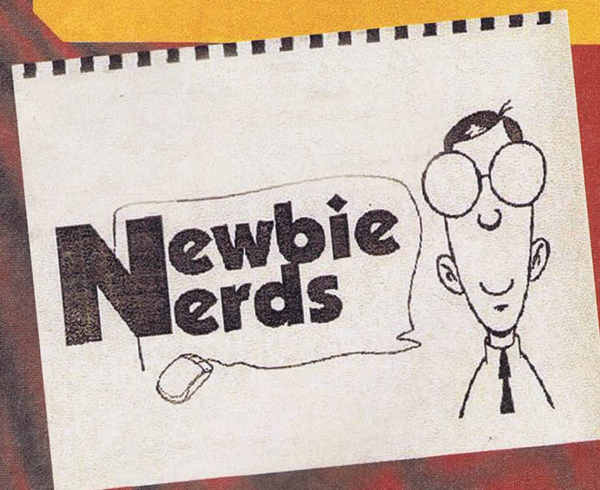
Michele "SoNiK©" Bruseghin
sonik.sniper@libero.it

LINK UTILI

Per testare Tracert e Whois:
www.samspade.org

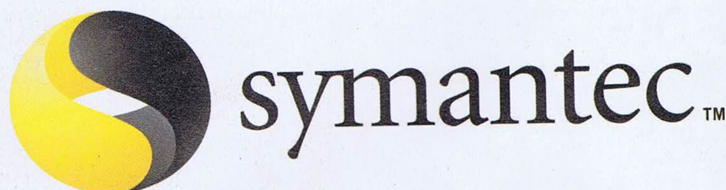
Database europeo NIC dei domini .it:
www.nic.it/RA/database/database.html

Whois domini .com, .net e .org testato nell'esempio:
www.networksolutions.com/es_US/whois/index.jhtml



SYMANTEC: bucatini software

Se chiamavamo spaghetti software il codice talmente intricato e malmesso da non riuscire neanche a leggerlo, i programmi pieni di buchi possono benissimo avere un nome simile...





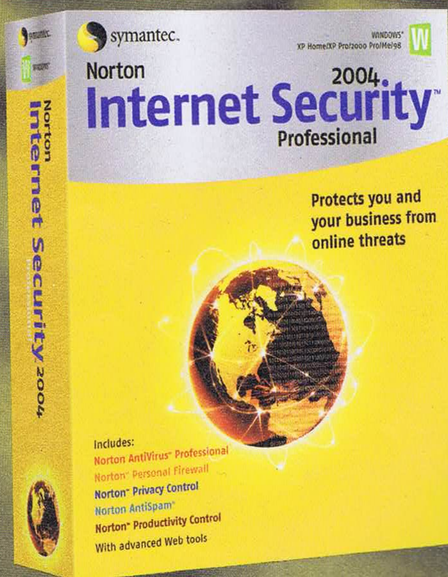
Ci siamo lasciati nello scorso numero di Hacker Journal alle prese con un programma dal nome altisonante di Norton Internet Security. E la scoperta che, secondo i criteri inseriti nel programma, il sito di Hacker Journal va bloccato, perché ricade nella categoria Crimine.

Dovrebbe bastare visitare http://www.hackerjournal.it, che avrà anche tanti difetti ma certamente non contiene niente di criminale, per rendersi conto di che cosa possano valere i criteri di Norton Internet cosiddetta-Security.

A parte questo, comunque, abbiamo deciso di provare un po' il programma e vedere se riserva altre sorprese oltre alle sue opinioni circa il nostro sito. La sorpresa è che, prima ancora di essere un pessimo programma di sicurezza, Norton Internet ti-vendo-la-Security è un programma problematico di suo. Su un sistema pulito abbiamo fatto un sacco di fatica a installare la demo, dopo vari errori e altrettanti tentativi andati a vuoto.

A programma installato... beh: non tutti sanno che l'edizione 2002 di questo programma aveva problemi nella parte di Personal Firewall aveva problemi con vari software, uno per tutti Infopop. Ecco, l'edizione 2004, tre versioni e due anni dopo, ha ancora esattamente lo stesso problema! Considerato che il programma dispone di un LiveUpdate che ci consente di scaricare una patch in tempo reale, quanti anni ci vorranno per rimediare a un problema riconosciuto?

> "Se avete un buon antivirus ed un OS aggiornato, tutte le patacche targate Norton, McAfee e altre menate, le potete lasciare sugli scaffali"
>
> da un forum di Punto Informatico

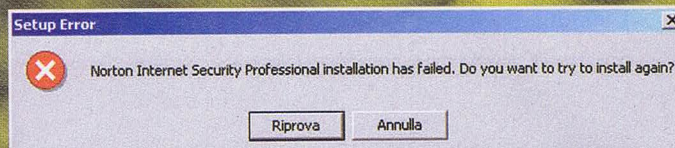


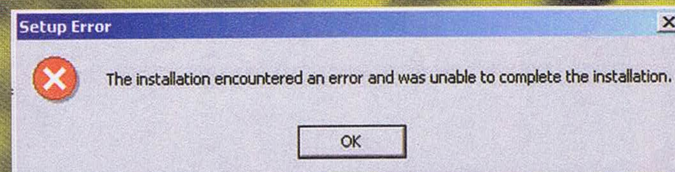
Un'altra bella scoperta che abbiamo fatto è questa: se abbiamo fatto un backup della macchina con Norton Ghost e poi abbiamo disinstallato quest'ultimo, il diabolico LiveUpdate insiste a scaricarne gli aggiornamenti... per un programma che non c'è più. Sulle connessioni veloci non è questo gran problema, ma appena manca un po' di banda si vede subito e francamente anche questo problema appare abbastanza sciocco. Per non parlare del nervoso che può venire ad aziende che magari comprano il

pacchetto in negozio e poi si ritrovano a scaricare qualche decina di mega di update per avere un prodotto aggiornato. Ogni tanto in Symantec potrebbero anche aggiornare i Master dei CD.

Il nostro verdetto

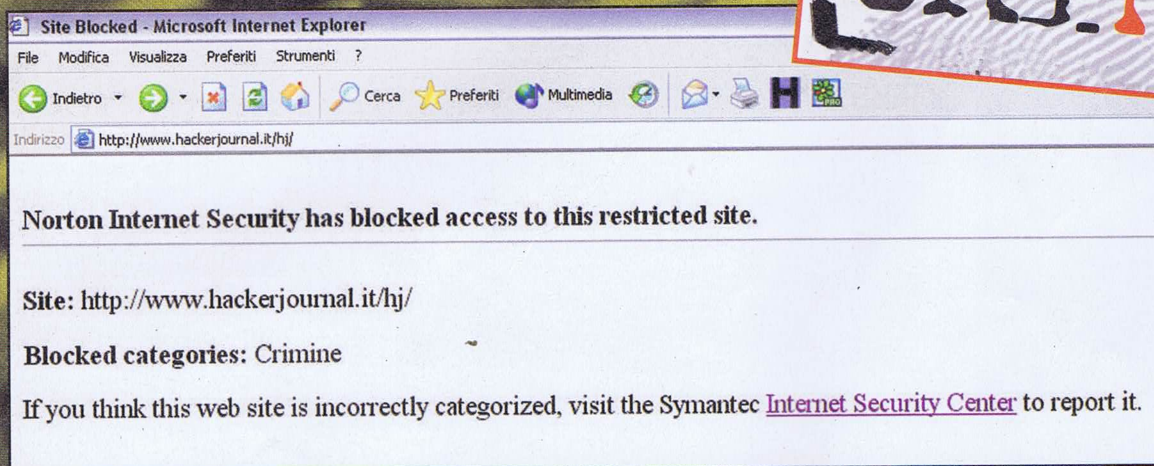
Installazione balbettante, bug noiosi che si trascinano da anni, incongruenze negli aggiornamenti, valutazione dei siti Internet da dimenticare… Norton Internet Security-forse è decisamente un programma da consigliare. A chi è disposto a sopportare fastidi peggiori dei rischi che il programma afferma di eliminare.





► La prima volta che abbiamo provato a installare la demo di Norton Internet presunta-Security su un PC pulito abbiamo ricevuto questi due utilissimi messaggio di errore.





◄ Il nostro sito, secondo le liste così ben curate da Symantec, appartiene alla categoria Crimine. Il loro software a che categoria appartiene?

AVANTI, (NORTON) È APERTO

Pochi giorni prima di chiudere la rivista, il sito di Secunia ha diffuso la descrizione di quattro vulnerabilità gravi scoperte da eEye Digital Security e presenti praticamente in tutte le versioni recenti di Norton Internet sedicente-Security.
Symantec ha pubblicato una patch da scaricare via il suo LiveUpdate, ovviamente. Ma qualcuno ha altro da fare oltre a verificare quotidianamente gli aggiornamenti e si ritrova in casa un software di sicurezza che in realtà ripara da worm e altre piacevolezze come un giornale vecchio sulla testa ripara da un temporale.

Le falle possono causare un attacco DoS (Denial of Service) se non addirittura consentire all'aggressore di prendere il controllo del computer:

1. Un boundary error all'interno del driver SYMDNS.SYS. Inviando a un sistema vulnerabile un responso NBNS (NetBIOS Name Service) fatti in un certo modo si può causare un buffer overflow ed eseguire, in certe condizioni, codice arbitrario che gira con gli stessi privilegi del kernel.

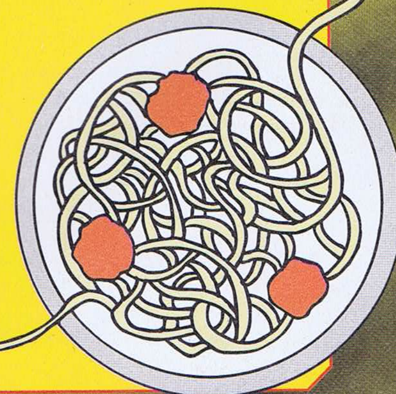
2. Allo stesso modo, attaccando il medesimo driver con responsi DNS ben costruiti si può portare il sistema al collasso.

3. La debolezza del driver rispetto all'elaborazione di NBNS può essere sfruttata anche per danneggiare lo heap e ancora una volta aprire le porte a processi malevoli che godono dei privilegi di kernel.

4. Questo buco è il più spettacolare di tutti. Un responso DNS contenente un nome canonico molto lungo nel campo CNAME di un record di risorsa permette di eseguire codice arbitrario con tutti i privilegi possibili anche se tutte le porte sono filtrate e vengono applicate tutte le regole antiintrusione.

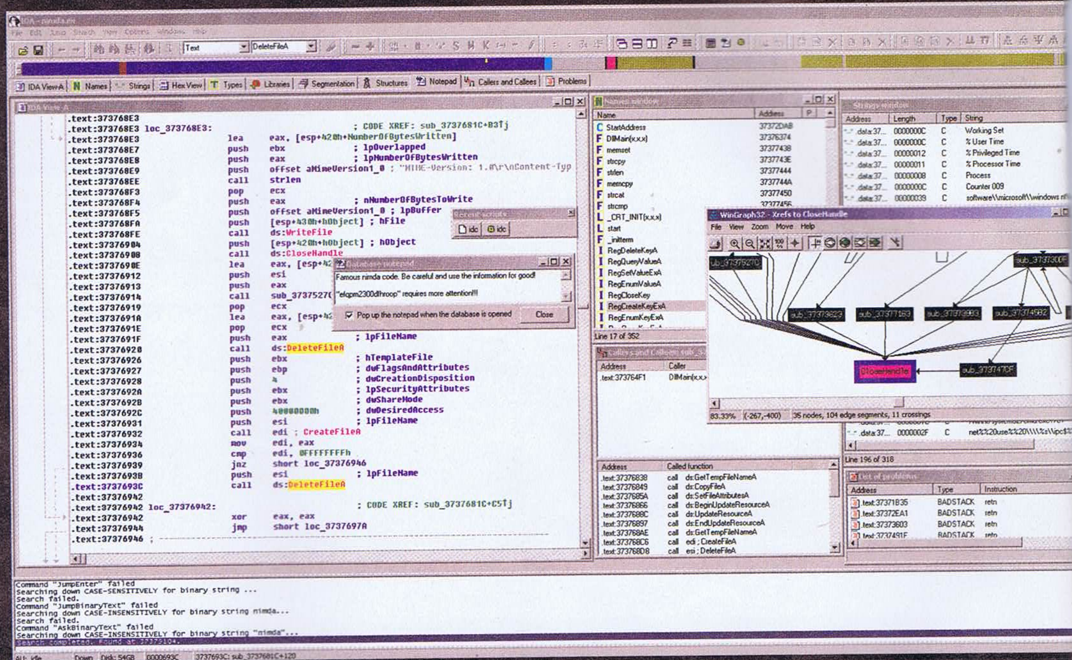
Questa vulnerabilità è stata definita “estremamente critica” perché spalanca il computer ai peggiori worm. Il problema è molto simile a quello che permetteva al worm Witty di farsi largo in un sistema approfittando di una falla del programma di chat ICQ.
Per un programma che contiene nel nome le parole Internet Security non è esattamente il massimo…

Tutti i dettagli si possono leggere sul sito http://secunia.com/advisories/11066.



COME FUNZIONANO I PROGRAMMI

Estirpiamo alla radice il malware con DLL fatte su misura per ingannarlo



▲ IDA è uno dei migliori disassemblatori sulla piazza, a http: //www.datarescue.com/idabase/



È sorprendente vedere quanti programmi usino Aureate/Radiate per inviarci pubblicità non richiesta. È sorprendente anche constatare i risultati che possiamo ottenere con un po' di programmazione.

Per replicare quanto detto in questo articolo servono un disassemblatore come IDA (http://www.datarescue.com/idabase/), strumenti di sviluppo software, per esempio gli SDK (Software Development Kit) di Microsoft, e un compilatore. Naturalmente bisogna avere competenze di programmazione; e per ultimo serve anche Ad-aware.

AD-AWARE
Simpatico programma che lavora per ripulire il disco rigido da tutte le forme di pubblicità indesiderata e in generale dai programmi che lavorano di nascosto e contro il nostro volere. http://www.lavasoft.de o http://www.lavasoftusa.com

Capire dove colpire

Una buona strategia per scoprire il punto debole dell'adware è installarlo e poi combatterlo con Ad-aware. Per esempio, scarichiamo NetAnts e poi debelliamolo con Ad-aware.

A questo punto, se proviamo ad attivare nuovamente NetAnts, darà un errore di tipo LoadLibrary(adimage.dll)[126]. Non è importante che appaia esattamente proprio questo errore, che dipende dalle versioni del software e potrebbe cambiare; il punto è leggerlo. In questo caso è evidente che la libreria vitale per gli interessi di NetAnts è adimage.dll. Reinstalliamo NetAnts in modo che funzioni e facciamo un backup della libreria in questione. Così possiamo condurre i nostri esperimenti sul backup e avere sempre l'originale pronto per un esperimento successivo.

Come chirurghi

Un veloce controllo delle dipendenze mostra che NetAnts non si collega implicitamente ad alcuna libreria di aureate/radiate. Allora lo disassembliamo con IDA. Cercando tutte le occorrenze di LoadLibrary, è evidente che NetAnts usa solo adimage.dll. Adesso lo freghiamo: scriviamo una nostra versione di adimage.dll che somiglia a quella vera, ma non permette al programma di rompere le scatole.

MALWARE
Tutti i programmi che fanno cose contro la nostra volontà, si installano senza che lo abbiamo permesso e in generale lavorano contro di noi. Dai virus ai programmi che inviano i nostri dati ad aziende pubblicitarie (adware).

MALEDETTI



CREIAMO UN FILEADIMAGE.C:

```
BOOL APIENTRY DllMain(HANDLE hMod,
DWORD dw, LPVOID lpV)
   {
      return TRUE;
   }
```

Usando Depends possiamo vedere tutte le funzioni esportate da adimage.dll e copiarne i nomi nel nostro file adimage.c. Dopo di che, per ciascuna funzione esportata, creiamo una funzione write come questa:

```
      DWORD Initialize ()
      {
          return 1;
      }
```

Ora dobbiamo sapere il numero giusto di parametri accettati dalla funzione. Disassemblando adimage.dll con IDA, cerchiamo la funzione desiderata e riceviamo tutte le informazioni che servono:

```
10002F6E
10002F6E ;            S u b r o u t i n e
10002F6E ; Attributes: bp-based frame
10002F6E
10002F6E              public Initialize
10002F6E Initialize      proc near       ; CODE
XREF: std_Initialize+1
10002F6E
10002F6E var_260        = byte ptr -260h
10002F6E var_15D        = byte ptr -15Dh
10002F6E var_15C        = byte ptr -15Ch
10002F6E var_58         = byte ptr -58h
10002F6E var_24         = byte ptr -24h
10002F6E var_4          = dword ptr -4
10002F6E arg_0          = dword ptr 8       <–
arg #1
10002F6E arg_4          = dword ptr 0Ch       .
10002F6E arg_8          = dword ptr 10h       .
10002F6E arg_C          = dword ptr 14h       .
10002F6E arg_10         = dword ptr 18h     <–
arg #5
10002F6E
10002F6E              push   ebp
10002F6F              mov    ebp, esp
10002F71              sub    esp, 260h
```

Initialize accetta cinque parametri (arg, da argument). Ecco come modifichiamo il codice C di prima:

```
 DWORD Initialize (DWORD a1, DWORD a2,
DWORD a3, DWORD a4, DWORD a5)
    {
      return 1;
    }
```

Ripetiamo la procedura per tutte le funzioni chiamate. Siccome, una volta linkate, alle variabili si fa riferimento tramite puntatori, possiamo ignorare il tipo C dei parametri originali.

Ora prepariamo un file DEF, adimage.def:

```
 LIBRARY     adimage

 EXPORTS

 Initialize         @1
 std_Initialize       @2
 StartMessaging       @3
 std_StartMessaging   @4
 SetThrottle          @5
 std_SetThrottle      @6
 SetProxy             @7
 std_SetProxy         @8
 Spuck                @9
 std_Spuck            @10
 SetOffline           @11
 std_SetOffline       @12
```

Compiliamo, linkiamo e inseriamo il file adimage.dll risultante nella directory di NetAnts.exe. Fatto!

La concorrenza

Se il successo ci dà alla testa e proviamo a fare la stessa cosa con Go!Zilla o NetVampire… non funzionerà. Ma è facile vedere, nello stesso modo di prima, che usano semplicemente DLL diverse, rispettivamente, tfde.dll e Advert.dll. Ricreando queste DLL come abbiamo fatto con adimage.dll tutto funziona… tranne loro! Grazie a garph0 per i suggerimenti.

Kurt Gödel
kurtgoedel@hackerjournal.it

Alcuni nemici tipici:
NetAnts (http://www.netants.com), NetVampire (http://www.netvampire.com), Go!Zilla (http://gozilla.com/).

AUREATE O RADIATE?

Aureate ha cambiato tempo fa il nome in Radiate per essere più pronunciabile dal pubblico americano, ma molte versioni del software continuano a identificarsi come Aureate. Nel dubbio, scriviamo sempre tutte e due le forme.

MAGICO

Sfruttando document.images, un array (vettore) indicizzato da un numero progressivo e contenente, nella sequenza in cui sono scritte nel codice sorgente HTML, tutte le immagini contenute nella pagina, possiamo così effettuare delle operazioni globali sulle immagini che ci sono in una pagina web.

La tecnica che utilizziamo è quella di cambiare in un sol colpo la classe CSS a tutte le immagini presenti sulla pagina. Tramite una classe CSS possiamo definire parecchi attributi grafici legati alle immagini. Così facendo, possiamo cambiare in un attimo molte proprietà delle immagini: infatti basta creare una classe CSS apposita da applicare come risultato della funzione. L'attributo javascript che definisce la classe di un oggetto è className.

```
<style>
.prima{height:100px}
.dopo{height:200px}
</style>
<script>
function cambia_classe(){
for(i=0;i<document.images.length;i++){
document.images[i].className="dopo"
}
}
</script>
```

richiamiamo la funzione come abbiamo visto in precedenza. Dobbiamo tener presente che questa tecnica non funziona qualora avessimo già settato altezza e larghezza tramite un CSS direttamente nel tag dell'immagine come in questo esempio

```
<img src="imma1.jpg" style="height:100px">
```

In questo caso prevale ciò che abbiamo dichiarato sul tag img, e l'immagine non si ridimensionerà. Purtroppo questa tecnica non funziona su Opera (perlomeno fino a Opera 6).

Da non confondere con Java, JavaScript infatti è un'altra cosa ed è proprietà di Netscape

Rendiamo migliori le nostre pagine web, con operazioni globali su tutte le immagini in JavaScript.

JAVASCRIPT



Immagini a tempo

Tramite questa tecnica possiamo caricare differenti immagini in base alla data (o all'ora), presente sul computer del visitatore. Anche in questo caso la mole di script in rete è immensa e per trovare qualcosa basta cercare. Vediamo un paio di esempi.

```
<script>
oggi=new Date()
img_mesi=new
Array("gen","feb","mar","apr","mag","giu","lug","ago","set","ott","nov","dic")
//Da ricordare lo slash alla fine
cartella="cartellaImmagini/"
estensione="jpg";
document.write("<img src=\""+cartella+img_mesi[oggi.getMonth()]+"."+esten-
sione+"\" alt=\""+img_mesi[oggi.getMonth()]+"\" />")
</script>
```

Nell'array img_mesi sono presenti i nomi delle immagini che andranno caricate di mese in mese. Attenzione: i nomi devono essere sprovvisti di estensione, che andiamo a settare alla riga successiva (questo per evitare di ripetere ogni volta l'estensione che probabilmente sarebbe la stessa), insieme al percorso relativo della cartella che contiene le immagini.
Possiamo usare lo stesso script per cambiare immagine ogni giorno, basta allungare l'array fino a 31 elementi e richiamarlo con oggi.getDate invece che con oggi.getMonth (parentesi comprese). Allo stesso modo, se vogliamo avere un'immagine differente per ogni giorno della settimana, dobbiamo richiamare l'array (avente in questo caso sette elementi), tramite oggi.getDay. Similmente possiamo agire per le ore (oggi.getHours) e in caso di necessità anche per i minuti (oggi.getMinutes).





E' semplice caricare un immagine con il mese in funzione della data

IMMAGINI IN BASE ALL'ORA DI GIORNATA (NOTTE, MATTINO, POMERIGGIO O SERA)

```
<script>
notte=new Array(23,6)
mattino=new Array(7,12)
pomeriggio=new Array(13,18)
sera=new Array(19,22)
oggi=new Date()
immagini=new Array("notte.jpg","mattina.jpg","pomeriggio.jpg","sera.gif")
img=""
if(oggi.getHours()>=notte[0] || oggi.getHours()<=notte[1]){
      img=immagini[0]
}
else if(oggi.getHours()>=mattino[0] && oggi.getHours()<=mattino[1]){
      img=immagini[1]
}
else if(oggi.getHours()>=pomeriggio[0] && oggi.getHours()<=pomeriggio[1]){
      img=immagini[2]
}
else{
      img=immagini[3]
}
document.write("<img src=\""+img+"\" alt=\""+img+"\" />");
</script>
```

In questo script dobbiamo settare solamente gli intervalli delle ore da considerare giorno, sera, notte e mattino, e l'array delle immagini da caricare, estensioni comprese.

IMMAGINI RANDOM

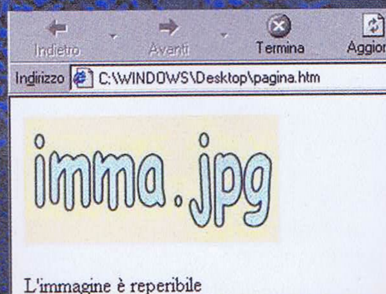
Per caricare un'immagine a caso scelta tra una lista, possiamo affidarci a uno script che, dato un array contenente un percorso di immagini, le carichi secondo un numero casuale ricavato tramite la funzione Math.random, che restituisce un numero casuale tra 0 e 1. Per questo motivo moltiplichiamo il risultato della suddetta funzione per il numero di immagini, ed estraiamo da questo risultato un numero intero (funzione parseInt)

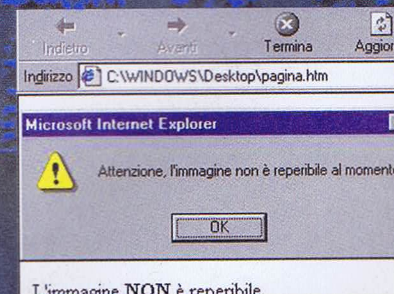
```
<script>
immagini= new Array()
immagini[0]="prima.jpg"
immagini[1]="seconda.jpg"
immagini[2]="terza.jpg"
random=parseInt(Math.random()*immagini.length)
document.write("<img src=\""+immagini[random]+"\" alt=\""+immagini[random]+"\" />")
</script>
```

PRELOAD DI IMMAGINI

Per gestire il caricamento di alcune immagini presenti su una pagina web prima di altre, possiamo affidarci a un semplice script che fa caricare al browser delle immagini presenti in un array javascript prima delle altre

```
<script>
immagini=new Array()
immagini[0]="prima.jpg"
immagini[1]="seconda.bmp"
immagini[2]="cartella/terza.gif"
arr_img=new Array()
for(i=0;i<immagini.length;i++){
      arr_img[i]=new Image()
      arr_img[i].src=immagini[i]
}
</script>
```





Tramite lo script prendiamo tutte le immagini presenti nel vettore "immagini", e configuriamo N oggetti Image() quante sono queste immagini. Per ogni oggetto, settiamo il parametro src, ovvero definiamo dove prendere l'immagine.

Controllo stato di raggiungibilità di un server o immagine. In caso di un controllo remoto, potrebbe essere utile sapere se un server esterno a quello del nostro sito è attivo o meno, per fare ciò possiamo utilizzare un metodo, poco ortodosso ma abbastanza versatile, che ci offre la gestione dell'evento onError su un'immagine presente nelle directory dell'altro server. Questa tecnica è anche utilizzabile per nascondere o caricare qualcosa di alternativo, nel caso l'immagine non fosse reperibile.

```
<img src="www.sito.it/immagine.jpg"
onError="
this.style.visibility='hidden';alert('Attenzione, questo server non è raggiungibile al momento')" />
```

Non facciamo altro che nascondere l'immagine e mostrare a video un messaggio.

Pederiva 'Dennis' Danilo

Rompiamo iTunes!

Dietro le quinte dell'ultimo caso di monopolio musicale, che mostra le prime crepe

Il 70% della musica venduta online, secondo le ultime statistiche, viene venduta dall'iTunes Music Store di Apple (http://www.apple.com/itunes/store/). Lo store è consultabile solo con il programma iTunes di Apple e anche le anteprime di trenta secondi, per vedere se un brano ci piace o meno, non si possono ascoltare senza iTunes.
Ma è così vero? No. Un giro a iTMS-4-ALL (http://itunes.punboy.net/cgi-bin/itms4all.pl) mostra che qualcuno sta sezionando il funzionamento dello store e presto potrebbe essere possibile spezzare il monopolio.

Presso la pagina http://hcsoftware.sourceforge.net/jasonrohrer/itms4all/ troviamo 250K di Perl che fanno funzionare il meccanismo. Per ora non è possibile acquistare brani, ma ci stanno lavorando su e un domani iTunes potrebbe diventare perfettamente inutile, consentendoci di usare il browser o il programma che vogliamo.

Questo si chiama software libero!

▲ *L'iTunes Music Store Apple si può usare solo con iTunes ...O no?*

INDIZI DI FUNZIONAMENTO

Non abbiamo spazio per analizzare esaustivamente il funzionamento dello store, ma alcune cose risultano chiare da subito:

- iTunes comunica con Apple quasi esclusivamente tramite HTTP, tranne che per l'autenticazione.
- I dati per mostrare la vetrina dello store e i risultati delle ricerche arrivano a iTunes come file XML compressi in gzip e cifrati con AES-128 (Rijndael) in modalità CBC.
- La chiave AES è 8a9dad399fb014c131be611820d78895.

◄ *Abbiamo cercato materiale dei Beastie Boys sull'iTunes Music Store... senza usare iTunes!*

CHIACCHIERE DIETRO ITUNES

Supponiamo di cercare materiale dei Beastie Boys. iTunes manda una richiesta HTTP come questa a phobos.apple.com sulla porta 80. User-Agent non può essere diverso da iTunes:

```
GET
/WebObjects/MZSearch.woa/wa/com.apple.jingle.search.DirectAction/search?term=Beastie%20Boys HTTP/1.1
User-Agent: iTunes/4.2 (Macintosh; U; PPC Mac OS X 10.2)
Accept-Language: en-us, en;q=0.50
Cookie: countryVerified=1
Accept-Encoding: gzip, x-aes-cbc
Connection: close
Host: phobos.apple.com
```

Apple risponde a iTunes con il seguente HTTP:

```
HTTP/1.1 200 Apple
Date: Fri, 16 Apr 2004 13:55:07 GMT
Content-Length: 4320
Content-Type: text/xml; charset=UTF-8
Cache-Control: no-cache
Connection: close
Server: Apache/1.3.27 (Darwin)
Pragma: no-cache
content-encoding: gzip, x-aes-cbc
x-apple-max-age: 3600
x-apple-crypto-iv: 19953b75e9846ea59715be906cdca0c8
x-apple-protocol-key: 2
x-apple-asset-version: 2118
x-apple-application-instance: 20
Via: 1.1 netcache04 (NetCache NetApp/5.2.1R3)

-- inizio dell'archivio cifrato --
```

Quando il GIOCO si fa DURO...

Se non sappiamo da dove cominciare per diventare hacker, forse è il caso di giocarci su!

Lo abbiamo sempre detto: non si diventa hacker leggendo un libro. Bisogna smanettare. Ma non è facile. Bisogna fare tanta fatica e accumulare grande esperienza, senza contare il rischio di combinare un guaio e finire indagati dalla polizia, o peggio.

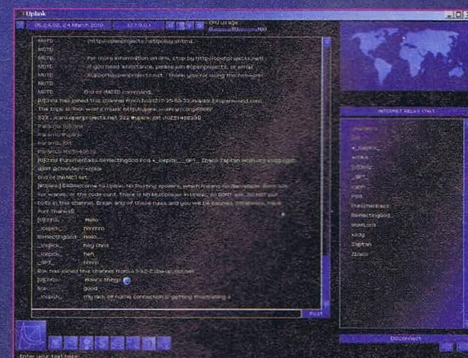
E allora perché non tenersi tutto il divertimento facendo a meno dei rischi? Per esempio giocando a fare gli hacker, in un ambito protetto e senza nessun rischio, ma con il gusto di tutte le sfide. Ci sono almeno due possibilità molto interessanti in quest'ambito: Street Hacker e Uplink. Tutti e due i giochi funzionano più o meno nello stesso modo. Abbiamo a disposizione un computer, una rete globale e qualche programma di quelli giusti. Possiamo decidere di agire da soli o per conto di una organizzazione e ci ritroveremo a dover fare veramente gli hacker. Ci sono password da scovare, sistemi in cui penetrare, blocchi da aggirare, codici segreti da scoprire, il tutto senza farsi scovare dagli amministratori di sistema e dalla polizia.



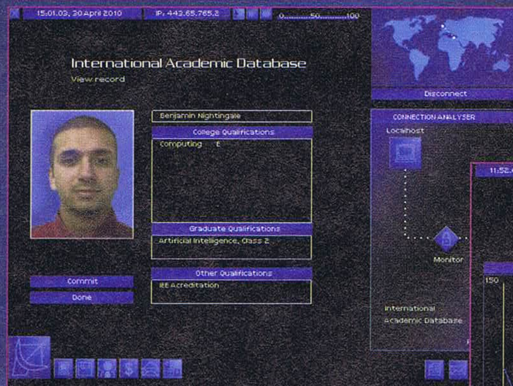
▲ Un worm usato all'interno di Street Hacker. Sta a noi maneggiarlo con cura e usarlo quando serve, dopo averlo creato o essercelo procurato, non sempre in modo ortodosso

Proseguendo nel gioco si diventa sempre più bravi e potenti, e i più intraprendenti possono anche autofinanziarsi mediante azioni, per così dire, di finanza creativa condotte tramite operazioni online presso banche internazionali. Sempre se riusciamo a fare le cose nel tempo giusto e nel modo giusto, e a schivare firewall e agenti di custodia.

Le missioni da compiere diventano progressivamente più difficili e sofisticate e richiedono strumenti sempre più evoluti. Il bello è che tutto è assolutamente simulato, virus, rete, password e sniffer compresi. Se commettiamo un errore non succede assolutamente niente e possiamo riprendere da dove abbiamo sbagliato.



▲ Anche nelle simulazioni, come Uplink, le conoscenze che scottano non si trovano tanto sul Web, quanto nelle stanze di chat di IRC



◄ Identikit di hacker, in Uplink.

► In Uplink si possono fare soldi in fretta con l'andamento della Borsa. Un bravo hacker può fare ancora più soldi...



◄ La nostra azione parte da Chicago, ma con Internet si arriva in fretta dappertutto. Chi sa riconoscere le altre città di questa mappa di Street Hacker?



▲ Un hacker di strada (appunto, street hacker) a volte si trova anche in situazioni d'azione, decisamente problematiche.

IMPEGNO ZERO: I WALLPAPER

Sia Uplink che Street Hacker offrono anche una bella raccolta di wallpaper, screensaver e perfino racconti a tema scritti dagli appassionati del gioco. Come dire che si può scoprire qualcosa di interessante anche solo visitando i siti.
In particolare sono da notare http://www.uplink.co.uk/otherfiles.html e http://downloads.streethacker.com/. Per Macintosh il link giusto è http://www.ambrosiasw.com/games/uplink/addons.html.I.

Soprattutto ci può anche capitare di violare la legge, ma per gioco, senza fare danni a niente e nessuno.
Qualcuno scuoterà le spalle. Sono giochi da bambini, un vero hacker di qui, un vero hacker di là, i lamer, questo e quello.



▲ I nodi critici della rete mondiale nella simulazione dannatamente appassionante.

Tutte stupidaggini. Tant'è vero che i piloti di aereo studiano per decine di ore sui simulatori, prima di decollare veramente. Se il simulatore è fatto bene, ci sono tutte le sfide e tutta l'adrenalina che uno si aspetta, ma zero rischi.

Questi sono fatti bene. L'invito è di provare davvero Street Hacker oppure Uplink.

STREET HACKER

http://www.streethacker.com

Demo gratuito parzialmente giocabile; il programma completo costa 25 dollari.
Per Windows (qualunque versione); serve il Net Framework 1.1 di Microsoft (http://windowsupdate.microsoft.com/).



▲ La scrivania dell'hacker high-tech (e high money)



▲ Accettiamo la missione?

Qualche livello di esperienza e chi vuole diventare hacker, ma non sa che cosa vuol dire o da dove cominciare, avrà le idee assai più chiare!

Nyarlathotep
nyarlathotep@hackerjournal.it

UPLINK

http://www.uplink.co.uk

Computer crime e spionaggio industriale sull'Internet del 2010.
Demo gratuito parzialmente giocabile; il programma completo costa 33,99 euro. È disponibile un Developer CD con dentro l'intero codice sorgente del gioco, a 44,99 euro.
Per Windows, Linux e Macintosh.

CYBERENIGMA SVELATO!

I RISULTATI DELLA SFIDA SUI PANGRAMMI

Sono arrivati programmi e pangrammi di tutti i colori, davvero! Complimenti a tutti. Nessun ha pensato di creare pangrammi con numeri romani, ma chi ha voglia può mandarli lo stesso...

Chi ha mandato programmi

Fabio (C, studiato al momento, soluzione semplice ma efficace), **Zerokool** (livello 11, programma bellissimo), **.:LoZ:.** in PHP, bello!, **X-3mE'89**, quasi completo. Possiamo trovare tutti i programmi nella Secret Zone del nostro sito!

Chi ha fatto a mano

Sigma5th e **Sara** sono riusciti a fare un pangramma di tredicesimo livello, bravi, **ETABETA** anche per lui livello 13, **Lorenzo "TADsince1995" Di Gaetano** dice che è impossibile. Naaa... **Stregatto** (livello 5 andando a crescere, bravo), **cypherbug** molto bravo con pangrammi autoreferenziali (livello 4), **Hack & Crack** livello 26, eccellente, **Surf3r** (26 in inglese e segnala http://www.rinkworks.com/words/autograms.shtml), **Tavano Mirko**, 14 anni, forza che puoi fare meglio! **doctor raquini turautau** (livello 26), **.:UFo_CuNi:.** livello 15, studia ogni tanto però! **Coky** livello 26, geniaccio, **Ribonix** cita Lee Sallows, **PaoloG** eccezionale, il migliore tanto da meritarsi un box a parte.

CHI NON CE L'HA FATTA

Space_1 ha scritto *Io non ho capito bene cosa si deve fare nel cyberenigma. Potete spiegarmelo meglio per favore?* **Max** ci ha preso in castagna: *Una cosina (da vero bastardo) la posso fare. Il pangramma di livello uno che proponete sul n° 49 è SBAGLIATO! Infatti "Questa frase contiene solo due lettere a" non è vera perché le lettere contenute sono 3...* non sei bastardo, sei preciso! Dovevamo esserlo anche noi. **torculus** ha visto lo stesso errore

IL PROGRAMMA DI .:LOZ:.

```
PAGINA 1 (index.php)

<html>

<head>
<meta http-equiv=""Content-Type"" con-
tent=""text/html; charset=iso-8859-1"">

</head>

<body>
<form name=""form1"" method=""post""
action=""result.php"">
  <textarea name=""frase""></textarea>
  frase<br>
<br>

  <select name=""dimensione"">
   <?php
          #creo un vettore con tutte le let-
tere dell'alfabeto
          $lettera = ""a b c d e f g h i j k l m n
o p q r s t u v w x y z"";
          $vett_lettera = explode("" "",$let-
tera);
          #creo un ciclo con la combo box a
cui corrisponde una dimensione numerica
per
ogni lettera scelta dell'alfabeto

          $z=1;
          for ($i=0;$i<26;$i++)
          {
                echo        ""<option
value=\""$z\"">$vett_lettera[$i]</option>"";
                $z++;
          }
          ?>
        </select>
 dimensione pangramma (fino a quale lette-
ra contare)<br>
<br>


  <input type=""submit"" name=""Submit""
value=""Submit"">
```

QUESTA ERA LA SFIDA

PANGRAMMA: FRASE CHE CONTA I CARATTERI CHE LA COMPONGONO

"Questa frase contiene solo tre lettere *a*" (pangramma di livello 1). "In queste virgolette si trovano tre *a* e una *b*" (livello 2). "Qua dentro si contano otto volte la *a*, una volta la *b* e due volte la *c*" (livello 3).

Per tutti: Che livello riesci a raggiungere?
Per esperti: Riesci a creare un pangramma di livello 21, con tutte le lettere dell'alfabeto italiano (abcdefghilmnopqrstuvz)?
Per geni: Riesci a creare un pangramma di livello 26, con tutte le lettere dell'alfabeto inglese (abcdefghijklmnopqrstuvwxyz)?

SORGENTI IN ARRIVO

Non abbiamo lo spazio per pubblicare tutti i sorgenti in queste due paginette, ma stiamo studiando una soluzione e daremo presto notizie! Intanto li abbiamo messi nella Secret Zone del sito, Gli autori che non fossero d'accordo ce lo possono segnalare e verranno rimossi immediatamente

Per super hacker: Riesci a scrivere un programma per creare pangrammi di qualsiasi livello?

Le regole...

La frase è libera. I numeri devono essere scritti in lettere. Le accentate contano come vocali normali (*à = a, è = e* eccetera).

IL PANGRAMMA DI LEE SALLOWS

LEE SALLOWS, GRANDE ENIGMISTA, HA COMPOSTO IL SEGUENTE PANGRAMMA:

Only the fool would take trouble to verify that his sentence was composed of ten a's, three b's, four c's, four d's, forty-six e's, sixteen f's, four g's, thirteen h's, fifteen i's, two k's, nine l's, four m's, twenty-five n's, twenty-four o's, five p's, sixteen r's, forty-one s's' thirty-seven t's, ten u's, eight v's, eight w's, four x's, eleven y's twenty-seven commas, twenty-three apostrophes, seven hyphens and, last but not least, a single

IL PANGRAMMA DI PAOLOG

Salve Hacker Journal, vi scrivo per dirvi che in questa frase ci sono trentasette a come ala, quattro b come babbo, quarantatre c come caso, quattordici d come dado, settantuno e come eco, tre f come foca, tre g come gru, quattro h come hotel, ventisette i come iena, tre j come juve, tre k come kevin, sette l come laguna, trentuno m come mano, ventisei n come neo, cinquantacinque o come oca, tre p come puma, dodici q come qui, ventotto r come ramo, quattordici s come scia, quarantatre t come tema, venticinque u come uva, tredici v come vino, due w come wurstel, due x come xeon, due y come yoda e due z come zorro

CHI HA GIOCATO AD ALTRO

Consoman89 scrive *ecco un pangramma di 21esimo livello: "per fare questa banale frase che leggerà molta gente ci ho messo zero numeri e tutte le ventuno lettere dell'alfabeto italiano"*. In realtà gioca a un altro gioco: chi è capace di scrivere la frase più corta possibile con dentro le ventuno lettere italiane? LeoX ha fatto meglio: *"queste virgolette hanno contenuto senza ampliamenti tutte le lettere dell'alfabeto italiano"*. ALIENz ha fatto ancora meglio: *mai posto quiz vaghi o indecifrabili.* ziodiegu lo ha fatto in inglese: *this crazy and beautifull phrase contain twenty-six enjoy letters of alphabet english and also very much mistake grammatical of quality.* C1n3770 scrive *In questa mail sono presenti tutte le lettere dell'alfabeto, senza aggiunta alcuna.* Jenova non ha capito bene il senso della sfida (o non abbiamo capito noi). blind manda il suo cyberenigma *Von Qzdsa zn fiqi!* Enrico Sunseri autoreferenzialissimo, Th3^CrOW ne manda cinque diversi, ftp21 attento alle consonanti, beppe caruso scrive *Ehi Fabio, un pomeriggio di questi andiamo a vedere Zeta la formica?*, lambaz ed Elia citano la celebre *The quick brown fox jumps over a lazy dog* (è la frase usata dai tipografi inglesi per visualizzare tutte le lettere), T1amat scrive *voglio che questo pangramma contenga l'alfabeto in una dozzina di parole,* 3mentina fa *ho decifrato bene il quiz, pagami se vuoi*

```
</form>
</body>
</html>

PAGINA 2 (result.php)

<html>
<head>
<meta http-equiv=""Content-Type"" content=""text/html; charset=iso-8859-1"">
</head>


<body>
<?php
#recupero gli elementi dalla pagina precedente
$frase = $_REQUEST['frase'];
$dimensione = $_REQUEST['dimensione'];

#rimpiazzo le lettere accentate con le vocali normali
$accenti = array(""Ö"",""ä"",""Ç"",""ç"",""ï"",""ó"");
$vocali = array(""a"",""e"",""e"",""i"",""o"",""u"");
$frase2 = str_replace($accenti, $vocali, $frase);

#creo un vettore con tutte le lettere dell'alfabeto completo
$lettere = ""a b c d e f g h i j k l m n o p q r s t u v w x y z"";
$vett_lettere = explode("" "",$lettere);

#tolgo gli spazi dalla frase
$frase2 = str_replace("" "","""", $frase2);

#con un espressione regolare perl trasformo la variabile frase in un vettore monodimensionale
$vett_frase = preg_split('//', $frase2, -1, PREG_SPLIT_NO_EMPTY);

#azzero il puntatore del vettore
reset ($vett_frase);

#creo due cicli annidati tenendo ferma la lettera dell'alfabeto e confrontandola
con ogni lettera della frase
#nel caso il confronto dia esito positivo incremento la variabile $cont che
conteggia il numero di lettere
for ($k=0;$k<$dimensione;$k++)
{
        $cont = 0;

        foreach ($vett_frase as $ff)
        {
                if ($ff == $vett_lettere[$k] || $ff == strtoupper($vett_lettere[$k]))
                {
$cont++;
                }//fine if

        }//fine foreach

        #controllo quante volte si ripete la lettera
        if ($cont == 1)
        {
        echo ""LA LETTERA "".$vett_lettere[$k]."" E' PRESENTE UNA SOLA VOLTA <br>"";
        }
        if ($cont > 1)
        {
        echo ""LA LETTERA "".$vett_lettere[$k]."" ESISTE $cont VOLTE <br>"";
        }

}//fine for

#stampo la frase originale
echo ""NELLA FRASE $frase"";
?>

</body>
</html>
```

.:LOZ:.

HACKER JOURNAL

IL PROSSIMO NUMERO IN EDICOLA IL 17 giugno 2004!

CYBERENIGMA

Il cifrario più sicuro al mondo è il cosiddetto one-time pad, cifrario usa e getta, perché è praticamente inviolabile. Il problema è trasmettere efficacemente la chiave e generarne una buona. Ecco un esempio molto banale

Questo è il messaggio da cifrare per la nostra amica Anita:

CI VEDIAMO AL CINEMA

La chiave è il suo nome: ANITA. Sovrapponiamo messaggio e codice:

CIVEDIAMOALCINEMA
ANITAANITAANITAAN

Spostiamo in avanti ogni lettera del messaggio secondo la chiave. Nell'alfabeto A = 1, N = 14, I = 9, T = 20. Quindi spostiamo la C avanti di 1, la I avanti di 14, la V avanti di 9 e così via. L'alfabeto si intende circolare; dopo la Z c'è di nuovo la A. Questo è il messaggio che passiamo ad Anita, dicendole sottovoce "la chiave è il tuo nome!":

DWEYEJOVIBMQRHFNO

Per decifrarlo, Anita applica il procedimento inverso:

DWEYEJOVIBMQRHFNO
ANITAANITAANITAAN

E usa la chiave spostando all'indietro le lettere (la D iniziale, indietro di A = 1, diventa una C e via dicendo).

Capito? Siamo pronti per il Cyberenigma!
Le regole: contiamo le accentate come se non lo fossero (à = a, è = e eccetera).
L'alfabeto è a 26 lettere (abcdefghijklmnopqrstuvwxyz).

✪ **Per tutti:** Se invece che a Anita scrivessimo a Samantha, usando il suo nome come chiave, come apparirebbe il messaggio in codice?

✪✪ **Per esperti:** Il messaggio è DJYLNDC-DALKBDMMLMJJYTVTPBEAPRRSAMTIKISM. La chiave è la testata del quattordicinale hacker più bello che c'è in edicola!

✪✪✪ **Per geni:** Il messaggio originale è SECONDO ME SI TRATTA DI UN CODICE INVIOLABILE. Il messaggio cifrato è UN HACKER NON SI FA FERMARE DA NIENTE E NESSUNO. Qual è una chiave possibile di codifica? Ne esiste una più corta?

✪✪✪✪ **Per super hacker:** Questo è un vero one-time pad. Le specifiche sono: algoritmo Arcfour e MD5. La chiave è cyberenigma. Il messaggio in codice è Ti7MhqTu4SvePxQXiw/J4xT0iD5jvIU2f6Rr90WHoRTXM+r5cHpa3MYDZSG78ZRbCWVex0SR2sEDLiCfpDA=. Qual è il messaggio originale?

Per chi è super hacker ma si sta disperando:
http://www.vidwest.com/crypt/.
Come al solito, però, c'è più gusto a fare da soli!

Le risposte a:

guestbook@hackerjournal.it